PCT/JP2004/011160

日本国特許庁
JAPAN PATENT OFFICE

05.08.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　８月　８日

出願番号
Application Number: 特願２００３－２９００５３
[ST. 10/C]: [ＪＰ２００３－２９００５３]

出願人
Applicant(s): ソニー株式会社

２００４年　５月２７日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０４５１５０

【書類名】　特許願
【整理番号】　0390222704
【提出日】　平成15年 8月 8日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　大森　睦弘
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　角田　智弘
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　嶌田　繁広
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082131
　【弁理士】
　【氏名又は名称】　稲本　義雄
　【電話番号】　03-3369-6479
【手数料の表示】
　【予納台帳番号】　032089
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9708842

【書類名】特許請求の範囲
【請求項１】
ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置であって、
前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示手段と、
前記提示手段により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定手段と、
前記他の情報処理装置を特定する特定手段と、
前記特定手段により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記提示手段は、音声、点字、または振動によりユーザに情報を提示する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項３】
準静電界通信、電磁波通信、光通信、または電気的通信を行う通信手段をさらに備える
ことを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記情報処理装置の外部の機器を、入力または出力のインタフェースとして利用する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記外部の機器と、準静電界通信、電磁波通信、光通信、または電気的通信を行う
ことを特徴とする請求項４に記載の情報処理装置。
【請求項６】
前記特定手段は、前記他の情報処理装置を、前記他の情報処理装置のURIに基づいて特定する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項７】
前記特定手段は、前記他の情報処理装置を特定する情報として、前記URIの一部分を設定するURI設定手段を備える
ことを特徴とする請求項６に記載の情報処理装置。
【請求項８】
前記他の情報処理装置と初回の通信を行うとき、前記他の情報処理装置に前記情報処理装置を特定する情報を送信する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項９】
前記他の情報処理装置と初回の通信を行うとき、前記他の情報処理装置を認証する合言葉を設定し、前記合言葉を前記他の情報処理装置に送信し、
前記他の情報処理装置と２回目以降の通信を行うとき、前記他の情報処理装置から送信された合言葉が、前記合言葉と一致するか否かを判定し、前記合言葉と一致すると判定された場合、前記他の情報処理装置との通信を継続し、前記合言葉と一致しないと判定された場合、前記他の情報処理装置との通信を拒絶する
ことを特徴とする請求項８に記載の情報処理装置。
【請求項１０】
前記他の情報処理装置と２回目以降の通信を行うとき、
前記他の情報処理装置は、前記情報処理装置から送信された合言葉が、前記合言葉と一致するか否かを判定し、前記合言葉と一致すると判定された場合、前記情報処理装置との通信を継続し、前記合言葉と一致しないと判定された場合、前記情報処理装置との通信を拒絶する

ことを特徴とする請求項９に記載の情報処理装置。
【請求項１１】
前記他の情報処理装置と初回の通信を行うとき、前記情報処理装置が情報を暗号化するために用いる第１のコードと、前記第１のコードに対応して生成される第２のコードを生成し、前記第１のコードを前記他の情報処理装置に送信し、
前記他の情報処理装置が情報を暗号化するために用いる第３のコードを前記通信手段を介して取得する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項１２】
前記他の情報処理装置と２回目以降の通信を行うとき、
前記情報処理装置は、前記他の情報処理装置を認証する任意の合言葉を設定し、前記合言葉を前記第３のコードで暗号化してチャレンジコードとして前記他の情報処理装置に送信し、
前記他の情報処理装置は、前記チャレンジコードを前記第３のコードに対応して生成される第４のコードで復号し、復号した前記チャレンジコードを前記第１のコードで暗号化してレスポンスコードとして前記情報処理装置に送信し、
前記情報処理装置は、前記レスポンスコードを前記第２のコードで復号し、
復号された前記レスポンスコードが、前記合言葉と一致するか否かを判定し、前記合言葉と一致すると判定された場合、前記他の情報処理装置との通信を継続し、前記合言葉と一致しないと判定された場合、前記他の情報処理装置との通信を拒絶する
ことを特徴とする請求項１１に記載の情報処理装置。
【請求項１３】
前記第１乃至第４のコードを同じコードとする
ことを特徴とする請求項１２に記載の情報処理装置。
【請求項１４】
前記他の情報処理装置と２回目以降の通信を行うとき、
前記他の情報処理装置は、前記情報処理装置を認証する任意の合言葉を設定し、前記合言葉を前記第１のコードで暗号化してチャレンジコードとして前記情報処理装置に送信し、
前記情報処理装置は、前記チャレンジコードを前記第２のコードで復号し、復号した前記チャレンジコードを前記第３のコードで暗号化してレスポンスコードとして前記他の情報処理装置に送信し、
前記他の情報処理装置は、前記レスポンスコードを前記第４のコードで復号し、
復号された前記レスポンスコードが、前記合言葉と一致するか否かを判定し、前記合言葉と一致すると判定された場合、前記情報処理装置との通信を継続し、前記合言葉と一致しないと判定された場合、前記情報処理装置との通信を拒絶する
ことを特徴とする請求項１２に記載の情報処理装置。
【請求項１５】
前記第２のコードは、前記情報処理装置の外部の機器に記憶され、
前記情報処理装置は、前記第２のコードが必要となったとき、前記外部の機器と通信し、前記第２のコードを取得し、前記第２のコードを取得した後、所定の時間が経過したとき、前記第２のコードを消去する
ことを特徴とする請求項１１に記載の情報処理装置。
【請求項１６】
前記他の情報処理装置を特定する情報、前記他の情報処理装置を認証するために必要な情報、および前記他の情報処理装置が前記情報処理装置を認証するために必要な情報を含むパッケージ情報を生成し、
前記ユーザの指定に基づいて、前記パッケージ情報を他の情報処理装置に送信する
ことを特徴とする請求項１１に記載の情報処理装置。
【請求項１７】

前記ユーザ情報を前記他の情報処理装置から提供されたコンテンツの利用履歴にもとづいて更新する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項１８】
前記ユーザ情報を管理する情報管理装置とネットワークを介して通信し、前記情報処理装置に記憶されたユーザ情報の内容が前記情報管理装置に記憶されたユーザ情報の内容と同じになるように前記ユーザ情報を更新する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項１９】
前記情報管理装置は、前記ユーザ情報の読み出しまたは変更が許可された前記他の情報処理装置を特定し、前記ユーザ情報を前記ユーザ情報の読み出しまたは変更が許可された他の情報処理装置に、前記ネットワークを介して提供する
ことを特徴とする請求項１８に記載の情報処理装置。
【請求項２０】
前記ユーザが所持する情報機器が発信する信号に基づいて、前記ユーザを認証する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項２１】
前記ユーザの体に発生する準静電界または静電界の変化パターンに基づいて、前記ユーザを認証する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項２２】
予め設定された時間内に、前記ユーザを認証できない場合、前記ユーザ情報を消去する
ことを特徴とする請求項２１に記載の情報処理装置。
【請求項２３】
前記ユーザ情報を消去した後、前記ユーザを認証できた場合、前記情報管理装置に記憶されているユーザ情報を前記ネットワークを介して取得する
ことを特徴とする請求項２２に記載の情報処理装置。
【請求項２４】
前記ユーザ情報は、前記ユーザの嗜好を表す嗜好情報を有し、
前記ユーザが指定する情報機器に前記嗜好情報を送信し、前記情報機器を前記嗜好情報に対応して動作させる
ことを特徴とする請求項１に記載の情報処理装置。
【請求項２５】
前記他の情報処理装置により提供される情報と、前記嗜好情報に基づいて前記情報機器を動作させる
ことを特徴とする請求項２４に記載の情報処理装置。
【請求項２６】
前記他の情報処理から送信された情報に基づいて、プログラムを実行する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項２７】
複数の他の情報処理装置に関連付けられた複数のユーザ情報に基づいて、あらたなユーザ情報を生成する
ことを特徴とする請求項１に記載の情報処理装置。
【請求項２８】
前記他の情報処理装置のプログラムを実装する
こと特徴とする請求項１に記載の情報処理装置。
【請求項２９】
ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置の情報処理方法であって、
前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示

ステップと、
　前記提示ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定ステップと、
　前記他の情報処理装置を特定する特定ステップと、
　前記特定ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶ステップと
　を含むことを特徴とする情報処理方法。
【請求項３０】
　ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置のプログラムであって、
　前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報の提示を制御する提示制御ステップと、
　前記提示制御ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可の指定を制御する指定制御ステップと、
　前記他の情報処理装置の特定を制御する特定制御ステップと、
　前記特定制御ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップと
　をコンピュータに実行させることを特徴とするプログラム。
【請求項３１】
　ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置のプログラムが記録される記録媒体であって、
　前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報の提示を制御する提示制御ステップと、
　前記提示制御ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可の指定を制御する指定制御ステップと、
　前記他の情報処理装置の特定を制御する特定制御ステップと、
　前記特定制御ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップと
　をコンピュータに実行させるプログラムが記録されることを特徴とする記録媒体。

【書類名】明細書
【発明の名称】情報処理装置および方法、プログラム、並びに記録媒体
【技術分野】
【０００１】
本発明は、ユーザの利便性を向上させ、さらにユーザにとって快適で安心なサービスを提供できるようにする情報処理装置および方法、プログラム、並びに記録媒体に関する。
【背景技術】
【０００２】
近年、個人情報を提示することで、様々なサービスを受けられるようになった。個人情報としては、名前、住所、嗜好情報、サービスへの認証情報、点数情報、他の人からもらった情報等さまざまな情報があげられる。
【０００３】
このような個人情報をカードに保存して持ち運び、ユーザが店に入ったとき、ショッピングカートに搭載されたカードリーダによりカードの情報が読み取られ、カードの情報に基づいて、広告を表示したり、場所案内、好みの商品のディスカウント情報などを表示する技術が提案されている（例えば、非特許文献１参照）。
【０００４】
また、個人情報を利用して、個人認証を行い、商品の購入、支払いなどの処理を便利にしようとする試みも行われている（例えば、特許文献１乃至３参照）。
【０００５】
特許文献１によれば、ユーザの端末で、商品コードを入力し（または、商品のバーコードを読み込み）、それをページャー等での遠隔通信によりパブリックなネットワークに接続を行い、自宅のPCまたはPCS NCC(Personal Communication Service Network Control Center）に転送し、PCS NCCでは商品コードから商品の値段等の情報をユーザの端末へ転送する。商品情報はユーザの端末にのみ表示され、購入の申し込みを行うと、実際の支払いが電子マネー等で処理される。
【０００６】
また、特許文献２は、離れたところから、財務情報を制御するプラットフォームを提供しようとするもので、財務情報の提供は銀行により行われる。また、銀行とノンバンクの間で銀行業務とは関係のないサービスも提供する。
【０００７】
特許文献３は、携帯電話を使って、電子財布、ワイヤレスPIN(personal identification number)パッド、および非接触型のスマートカードの機能を実現しようというものである。携帯電話会社等でのサービスプロバイダーにおいて、アカウントと認証情報を保持し、携帯電話から予め決められた機能コードを入力すると、機能コードがサービスプロバイダーへ転送され要求された処理が行われる。サービスプロバイダーの中央処理装置により、認証が必要か否かの判断を行い、必用であれば個人認証番号を中央処理装置に転送し、中央処理装置にて認証処理を行い取引が行われる。
【０００８】
【非特許文献１】US2002-174025-A1　Method and System for providing targeted Advertising and personalized customer services (IBM)
【特許文献１】US5,991,601(Personal intercommunication purchase and fulfillment system)
【特許文献２】US5,787,403 (Bank-centric service platform, network and system)
【特許文献３】US5,991,749 (Wireless telephony for collecting tolls, conducting financial transactions, and authorizing other activities)
【発明の開示】
【発明が解決しようとする課題】
【０００９】

しかしながら、非特許文献１の技術では、他の店で受けたサービスとの情報交換ができない。また、カードを使っているのがユーザ本人か否かを確認する、なりすまし防止機構がないという課題があった。

【００１０】

また、特許文献１の技術では、PCS NCCにおいてデータベースの管理を行うにあたり、商品コードから商品情報を検索するためのデータベース作成等が必要になり、迅速な処理ができないという課題があった。

【００１１】

特許文献２の技術では、サービスの流れを規定しているが、ユーザの端末においてどのような認証処理がなされるかが考慮されていないという課題があった。

【００１２】

特許文献３の技術では、固定的な機能コードが必要となるため、認証システムおよび商品情報に依存した携帯電話等を作成しなければならず、柔軟なシステムの運用が行えず、その結果、ユーザの利便性が損なわれる恐れがあるという課題があった。

【００１３】

本発明はこのような状況に鑑みてなされたものであり、ユーザの利便性を向上させ、さらにユーザにとって快適で安心なサービスを提供できるようにするものである。

【課題を解決するための手段】

【００１４】

本発明の情報処理装置は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置であって、他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示手段と、提示手段により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定手段と、他の情報処理装置を特定する特定手段と、特定手段により特定された他の情報処理装置と他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶手段とを備えることを特徴とする。

【００１５】

前記提示手段は、音声、点字、または振動によりユーザに情報を提示するようにすることができる。

【００１６】

準静電界通信、電磁波通信、光通信、または電気的通信を行う通信手段をさらに備えるようにすることができる。

【００１７】

前記情報処理装置の外部の機器を、入力または出力のインタフェースとして利用するようにすることができる。

【００１８】

前記外部の機器と、準静電界通信、電磁波通信、光通信、または電気的通信を行うようにすることができる。

【００１９】

前記特定手段は、他の情報処理装置を、他の情報処理装置のURIに基づいて特定するようにすることができる。

【００２０】

前記特定手段は、他の情報処理装置を特定する情報として、URIの一部分を設定するURI設定手段を備えるようにすることができる。

【００２１】

前記他の情報処理装置と初回の通信を行うとき、他の情報処理装置に情報処理装置を特定する情報を送信するようにすることができる。

【００２２】

前記他の情報処理装置と初回の通信を行うとき、他の情報処理装置を認証する合言葉を設定し、合言葉を他の情報処理装置に送信し、他の情報処理装置と２回目以降の通信を行うとき、他の情報処理装置から送信された合言葉が、合言葉と一致するか否かを判定し、

合言葉と一致すると判定された場合、他の情報処理装置との通信を継続し、合言葉と一致しないと判定された場合、他の情報処理装置との通信を拒絶するようにすることができる。

【００２３】

前記他の情報処理装置と２回目以降の通信を行うとき、他の情報処理装置は、情報処理装置から送信された合言葉が、合言葉と一致するか否かを判定し、合言葉と一致すると判定された場合、情報処理装置との通信を継続し、合言葉と一致しないと判定された場合、情報処理装置との通信を拒絶するようにすることができる。

【００２４】

前記他の情報処理装置と初回の通信を行うとき、情報処理装置が情報を暗号化するために用いる第１のコードと、第１のコードに対応して生成される第２のコードを生成し、第１のコードを他の情報処理装置に送信し、他の情報処理装置が情報を暗号化するために用いる第３のコードを前記通信手段を介して取得するようにすることができる。

【００２５】

前記他の情報処理装置と２回目以降の通信を行うとき、情報処理装置は、他の情報処理装置を認証する任意の合言葉を設定し、合言葉を第３のコードで暗号化してチャレンジコードとして他の情報処理装置に送信し、他の情報処理装置は、チャレンジコードを第３のコードに対応して生成される第４のコードで復号し、復号したチャレンジコードを第１のコードで暗号化してレスポンスコードとして情報処理装置に送信し、情報処理装置は、レスポンスコードを第２のコードで復号し、復号されたレスポンスコードが、合言葉と一致するか否かを判定し、合言葉と一致すると判定された場合、他の情報処理装置との通信を継続し、合言葉と一致しないと判定された場合、他の情報処理装置との通信を拒絶するようにすることができる。

【００２６】

前記第１乃至第４のコードを同じコードとすることができる。

【００２７】

前記他の情報処理装置と２回目以降の通信を行うとき、他の情報処理装置は、情報処理装置を認証する任意の合言葉を設定し、合言葉を第１のコードで暗号化してチャレンジコードとして情報処理装置に送信し、情報処理装置は、チャレンジコードを第２のコードで復号し、復号したチャレンジコードを第３のコードで暗号化してレスポンスコードとして他の情報処理装置に送信し、他の情報処理装置は、レスポンスコードを第４のコードで復号し、復号されたレスポンスコードが、合言葉と一致するか否かを判定し、合言葉と一致すると判定された場合、情報処理装置との通信を継続し、合言葉と一致しないと判定された場合、情報処理装置との通信を拒絶するようにすることができる。

【００２８】

前記第２のコードは、情報処理装置の外部の機器に記憶され、情報処理装置は、第２のコードが必要となったとき、外部の機器と通信し、第２のコードを取得し、第２のコードを取得した後、所定の時間が経過したとき、第２のコードを消去するようにすることができる。

【００２９】

前記他の情報処理装置を特定する情報、他の情報処理装置を認証するために必要な情報、および他の情報処理装置が情報処理装置を認証するために必要な情報を含むパッケージ情報を生成し、ユーザの指定に基づいて、パッケージ情報を他の情報処理装置に送信するようにすることができる。

【００３０】

前記ユーザ情報を前記他の情報処理装置から提供されたコンテンツの利用履歴にもとづいて更新するようにすることができる。

【００３１】

前記ユーザ情報を管理する情報管理装置とネットワークを介して通信し、情報処理装置に記憶されたユーザ情報の内容が情報管理装置に記憶されたユーザ情報の内容と同じにな

るようにユーザ情報を更新するようにすることができる。

【００３２】

前記情報管理装置は、ユーザ情報の読み出しまたは変更が許可された他の情報処理装置を特定し、ユーザ情報をユーザ情報の読み出しまたは変更が許可された他の情報処理装置に、ネットワークを介して提供するようすることができる。

【００３３】

前記ユーザが所持する情報機器が発信する信号に基づいて、ユーザを認証するようにすることができる。

【００３４】

前記ユーザの体に発生する準静電界または静電界の変化パターンに基づいて、前記ユーザを認証するようにすることができる。

【００３５】

予め設定された時間内に、ユーザを認証できない場合、ユーザ情報を消去するようにすることができる。

【００３６】

前記ユーザ情報を消去した後、ユーザを認証できた場合、情報管理装置に記憶されているユーザ情報をネットワークを介して取得するようにすることができる。

【００３７】

前記ユーザ情報は、ユーザの嗜好を表す嗜好情報を有し、ユーザが指定する情報機器に嗜好情報を送信し、情報機器を嗜好情報に対応して動作させるようにすることができる。

【００３８】

前記他の情報処理装置により提供される情報と、嗜好情報に基づいて情報機器を動作させるようにすることができる。

【００３９】

前記他の情報処理から送信された情報に基づいて、プログラムを実行するようにすることができる。

【００４０】

複数の他の情報処理装置に関連付けられた複数のユーザ情報に基づいて、あらたなユーザ情報を生成するようにすることができる。

【００４１】

前記他の情報処理装置のプログラムを実装するようにすることができる。

【００４２】

本発明の情報処理方法は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置の情報処理方法であって、他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示ステップと、提示ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定ステップと、他の情報処理装置を特定する特定ステップと、特定ステップの処理により特定された他の情報処理装置と他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶ステップとを含むことを特徴とする。

【００４３】

本発明のプログラムは、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置と通信を行う情報処理装置のプログラムであって、他の情報処理装置により読み出しまたは変更が行われるユーザ情報の提示を制御する提示制御ステップと、提示制御ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可の指定を制御する指定制御ステップと、他の情報処理装置の特定を制御する特定制御ステップと、特定制御ステップの処理により特定された他の情報処理装置と他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップとをコンピュータに実行させることを特徴とする。

【００４４】

本発明の記録媒体は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置

と通信を行う情報処理装置のプログラムが記録される記録媒体であって、他の情報処理装置により読み出しまたは変更が行われるユーザ情報の提示を制御する提示制御ステップと、提示制御ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可の指定を制御する指定制御ステップと、他の情報処理装置の特定を制御する特定制御ステップと、特定制御ステップの処理により特定された他の情報処理装置と他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップとをコンピュータに実行させるプログラムが記録されることを特徴とする。

【００４５】

本発明の情報処理装置および方法、並びにプログラムにおいては、他の情報処理装置により読み出しまたは変更が行われるユーザ情報が提示され、提示されたユーザ情報の読み出しまたは変更の許可が指定され、他の情報処理装置が特定され、特定された他の情報処理装置と他の情報処理装置により読み出しまたは変更が行われるユーザ情報が関連付けられて記憶される。

【発明の効果】

【００４６】

本発明によれば、ユーザに利便性の高いサービスを提供することができる。特に、ユーザにとって快適で安心なサービスを提供できる

【発明を実施するための最良の形態】

【００４７】

以下に本発明の実施の形態を説明するが、本明細書に記載した発明と、発明の実施の形態との対応関係を例示すると、次のようになる。この記載は、本明細書に記載されている発明をサポートする実施の形態が明細書に記載されていることを確認するためのものである。従って、明細書には記載されているが、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その発明に対応するものではないことを意味するものではない。逆に、実施の形態が発明に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その発明以外の発明には対応しないものであることを意味するものでもない。

【００４８】

さらに、この記載は、明細書に記載されている発明が、全て請求されていることを意味するものではない。換言すれば、この記載は、明細書に記載されている発明であって、この出願では請求されていない発明の存在、すなわち、将来、分割出願されたり、補正により出願、または追加される発明の存在を否定するものではない。

【００４９】

本発明の情報処理装置は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置（例えば、図１のサービスシステム２４）と通信を行う情報処理装置（例えば、図１のＰＫ２２）であって、前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示手段（例えば、図４の許可項目確認モジュール６３）と、前記提示手段により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定手段（例えば、図４のユーザ制御許可入力モジュール６２）と、前記他の情報処理装置を特定する特定手段（例えば、図５のステップＳ１０２の処理を実行する図４のＤＢアクセスモジュール）と、前記特定手段により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶手段（例えば、図９のステップＳ８０５の処理を実行する図４のＤＢアクセスモジュール６６）とを備えることを特徴とする。

【００５０】

この情報処理装置は、準静電界通信、電磁波通信、光通信、または電気的通信を行う通信手段（例えば、図２の通信部１０９）をさらに備える。

【００５１】

この情報処理装置は、前記情報処理装置の外部の機器（例えば、図１５の外部コンソール２２１または２２２）を、入力または出力のインタフェースとして利用する。

【００５２】
この情報処理装置は、前記外部の機器と、準静電界通信、電磁波通信、光通信、または電気的通信を行う。
【００５３】
この情報処理装置は、前記特定手段は、前記他の情報処理装置を、前記他の情報処理装置のURIに基づいて特定する（例えば、図１０のサービスＩＤマッチング処理）。
【００５４】
この情報処理装置は、前記特定手段が、前記他の情報処理装置を特定する情報（例えば、サービスＩＤ）として、前記URIの一部分を設定するURI設定手段（例えば、図９のステップＳ８０４の処理を実行する図４のＤＢアクセスモジュール６６）を備える。
【００５５】
この情報処理装置は、前記他の情報処理装置と初回の通信を行うとき、前記他の情報処理装置に前記情報処理装置を特定する情報（例えば、ユーザＩＤ）を送信する。
【００５６】
この情報処理装置は、前記他の情報処理装置と初回の通信を行うとき、前記他の情報処理装置を認証する合言葉を設定し、前記合言葉を前記他の情報処理装置に送信し、前記他の情報処理装置と２回目以降の通信を行うとき、前記他の情報処理装置から送信された合言葉が、前記合言葉と一致するか否かを判定し（例えば、図６のステップＳ２８５）、前記合言葉と一致すると判定された場合、前記他の情報処理装置との通信を継続し、前記合言葉と一致しないと判定された場合、前記他の情報処理装置との通信を拒絶する。
【００５７】
この情報処理装置は、前記他の情報処理装置と２回目以降の通信を行うとき、前記他の情報処理装置は、前記情報処理装置から送信された合言葉が、前記合言葉と一致するか否かを判定し（例えば、図６のステップＳ２０４）、前記合言葉と一致すると判定された場合、前記情報処理装置との通信を継続し、前記合言葉と一致しないと判定された場合、前記情報処理装置との通信を拒絶する。
【００５８】
この情報処理装置は、前記他の情報処理装置と初回の通信を行うとき、前記情報処理装置が情報を暗号化するために用いる第１のコード（例えば、ＰＫの公開鍵）と、前記第１のコードに対応して生成される第２のコード（例えば、ＰＫの秘密鍵）を生成し、前記第１のコードを前記他の情報処理装置に送信し、前記他の情報処理装置が情報を暗号化するために用いる第３のコード（例えば、サービスシステムの公開鍵）を前記通信手段を介して取得する。
【００５９】
この情報処理装置は、前記他の情報処理装置と２回目以降の通信を行うとき、前記情報処理装置は、前記他の情報処理装置を認証する任意の合言葉を設定し、前記合言葉を前記第３のコードで暗号化してチャレンジコードとして前記他の情報処理装置に送信し（例えば、図７のステップＳ４８４）、前記他の情報処理装置は、前記チャレンジコードを前記第３のコードに対応して生成される第４のコード（例えば、サービスシステムの秘密鍵）で復号し、復号した前記チャレンジコードを前記第１のコードで暗号化してレスポンスコードとして前記情報処理装置に送信し（例えば、図７のステップＳ４０３）、前記情報処理装置は、前記レスポンスコードを前記第２のコードで復号し、復号された前記レスポンスコードが、前記合言葉と一致するか否かを判定し（例えば、図７のステップＳ４８７の処理）、前記合言葉と一致すると判定された場合、前記他の情報処理装置との通信を継続し、前記合言葉と一致しないと判定された場合、前記他の情報処理装置との通信を拒絶する。
【００６０】
この情報処理装置は、前記第１乃至第４のコードを同じコード（例えば、共通鍵）とする。
【００６１】

この情報処理装置は、前記他の情報処理装置と２回目以降の通信を行うとき、前記他の情報処理装置は、前記情報処理装置を認証する任意の合言葉を設定し、前記合言葉を前記第１のコードで暗号化してチャレンジコードとして前記情報処理装置に送信し（例えば、図７のステップＳ４０６）、前記情報処理装置は、前記チャレンジコードを前記第２のコードで復号し、復号した前記チャレンジコードを前記第３のコードで暗号化してレスポンスコードとして前記他の情報処理装置に送信し（例えば、図７のステップＳ４９０）、前記他の情報処理装置は、前記レスポンスコードを前記第４のコードで復号し、復号された前記レスポンスコードが、前記合言葉と一致するか否かを判定し（例えば、図７のステップＳ４０８）、前記合言葉と一致すると判定された場合、前記情報処理装置との通信を継続し、前記合言葉と一致しないと判定された場合、前記情報処理装置との通信を拒絶する。

【００６２】

この情報処理装置は、前記第２のコードが、前記情報処理装置の外部（例えば、図１のＳＢ２６）の機器に記憶され、前記情報処理装置は、前記第２のコードが必要となったとき、前記外部の機器と通信し、前記第２のコードを取得し（例えば、図８のステップＳ６８１）、前記第２のコードを取得した後、所定の時間が経過したとき、前記第２のコードを消去する（例えば、図８のステップＳ６８３）。

【００６３】

この情報処理装置は、前記他の情報処理装置を特定する情報、前記他の情報処理装置を認証するために必要な情報、および前記他の情報処理装置が前記情報処理装置を認証するために必要な情報を含むパッケージ情報（例えば、図２４のコンテンツアクセスパッケージ３６１）を生成し、前記ユーザの指定に基づいて、前記パッケージ情報を他の情報処理装置（例えば、図２４の端末２６）に送信する。

【００６４】

この情報処理装置は、前記ユーザ情報を前記他の情報処理装置から提供されたコンテンツの利用履歴にもとづいて更新する（例えば、図２１のＰＭＤ更新処理）。

【００６５】

この情報処理装置は、前記ユーザ情報を管理する情報管理装置（例えば、図１のｐＢａｓｅ２３）とネットワークを介して通信し、前記情報処理装置に記憶されたユーザ情報の内容が前記情報管理装置に記憶されたユーザ情報の内容と同じになるように前記ユーザ情報を更新する（例えば、図３０のステップS２００３）。

【００６６】

この情報処理装置は、前記情報管理装置が、前記ユーザ情報の読み出しまたは変更が許可された前記他の情報処理装置を特定し（例えば、図１８のステップS１１２２、または図１９のステップS１８８２）、前記ユーザ情報を前記ユーザ情報の読み出しまたは変更が許可された他の情報処理装置に、前記ネットワークを介して提供する（例えば、図１８のステップS１１２８または図１９のステップS１８９２）。

【００６７】

この情報処理装置は、前記ユーザが所持する情報機器（例えば、図１１Ａのチップ２０１）が発信する信号に基づいて、前記ユーザを認証する（例えば、図１２のユーザ認証処理１）。

【００６８】

この情報処理装置は、前記ユーザの体に発生する準静電界または静電界の変化パターン（例えば、図１１Ｂの歩紋２０２）に基づいて、前記ユーザを認証する（例えば、図１３のユーザ認証処理２）。

【００６９】

この情報処理装置は、予め設定された時間内に、前記ユーザを認証できない場合、前記ユーザ情報を消去する（例えば、図１４のステップＳ９４４）。

【００７０】

この情報処理装置は、前記ユーザ情報を消去した後、前記ユーザを認証できた場合、前

記情報管理装置に記憶されているユーザ情報を前記ネットワークを介して取得する（例えば、図１４のステップＳ９４１）。

【００７１】

この情報処理装置は、前記ユーザ情報が、前記ユーザの嗜好を表す嗜好情報を有し、前記ユーザが指定する情報機器（例えば、図２５の音楽再生装置３８１またはパーソナルコンピュータ３８２）に前記嗜好情報を送信し、前記情報機器を前記嗜好情報に対応して動作させる（例えば、図２５のパーソナライズ）。

【００７２】

この情報処理装置は、前記他の情報処理装置（例えば、図６０の協調フィルタリングサーバ１２０１）により提供される情報と、前記嗜好情報に基づいて前記情報機器を動作させる。

【００７３】

この情報処理装置は、前記他の情報処理から送信された情報に基づいて、プログラムを実行する（例えば、図４９のＰＫの処理）。

【００７４】

この情報処理装置は、複数の他の情報処理装置に関連付けられた複数のユーザ情報に基づいて、あらたなユーザ情報（例えば、図２２のＰＭＤ３０３）を生成する。

【００７５】

この情報処理装置は、前記他の情報処理装置のプログラム（例えば、図５９のサービスシステム２４－２０のプログラム）を実装する。

【００７６】

本発明の情報処理方法は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置（例えば、図１のサービスシステム２４）と通信を行う情報処理装置（例えば、図１のＰＫ２２）の情報処理方法であって、前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を提示する提示ステップ（例えば、図５のステップＳ４２）と、前記提示ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可を指定する指定ステップ（例えば、図５のステップＳ６３）と、前記他の情報処理装置を特定する特定ステップ（例えば、図５のステップＳ１０２）と、前記特定ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶する記憶ステップ（例えば、図９のステップＳ８０５）とを含む。

【００７７】

本発明のプログラムは、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置（例えば、図１のサービスシステム２４）と通信を行う情報処理装置（例えば、図１のＰＫ２２）のプログラムであって、前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報の提示を制御する提示制御ステップ（例えば、図５のステップＳ４２）と、前記提示制御ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可の指定を制御する指定制御ステップ（例えば、図５のステップＳ６３）と、前記他の情報処理装置の特定を制御する特定制御ステップ（例えば、図５のステップＳ１０２）と、前記特定制御ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップ（例えば、図９のステップＳ８０５）とをコンピュータに実行させる。

【００７８】

本発明の記録媒体は、ユーザに関連するユーザ情報を記憶し、複数の他の情報処理装置（例えば、図１のサービスシステム２４）と通信を行う情報処理装置（例えば、図１のＰＫ２２）のプログラムが記録される記録媒体であって、前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報の提示を制御する提示制御ステップ（例えば、図５のステップＳ４２）と、前記提示制御ステップの処理により提示されたユーザ情報の読み出しまたは変更の許可の指定を制御する指定制御ステップ（例えば、図５のステップＳ６

３）と、前記他の情報処理装置の特定を制御する特定制御ステップ（例えば、図５のステップＳ１０２）と、前記特定制御ステップの処理により特定された前記他の情報処理装置と前記他の情報処理装置により読み出しまたは変更が行われるユーザ情報を関連付けて記憶するように制御する記憶制御ステップ（例えば、図９のステップＳ８０５）とをコンピュータに実行させるプログラムが記録される。

【００７９】

以下、図面を参照して、本発明の実施の形態について説明する。図１は、本発明を適用したサービス提供システム１の構成例を表すブロック図である。この例においては、ユーザ２０が、そのユーザの個人関連情報を記憶する携帯可能な小型のコンピュータなどで構成されるＰＫ（Personal Key）２２を携帯している。ここで、個人関連情報とは、単に、名前、住所などそのユーザを特定するための情報だけでなく、嗜好情報、認証情報、点数情報、他の人からもらった情報などを含む、そのユーザに関連する様々な情報の集合を意味する。

【００８０】

ＰＫ２２は、アクセスポイント２５の周囲のエリア４１において、ＲＦ（Radio Frequency）通信、準静電界通信、光通信などの無線通信により、インターネット２１に接続されたアクセスポイント２５と通信する。また、ＰＫ２２は、無線通信などにより近傍の情報機器との通信も行う。ＰＫ２２は、暗号鍵に基づいて情報を暗号化する暗号化機能を有しており、暗号鍵の鍵データは必要に応じてＳＢ（Secure Button）２６に記憶される。ＳＢ２６は通信機能を有するコンピュータであり、ＰＫ２２と通信し、鍵データの送受信を行う。

【００８１】

インターネット２１には、ＰＫ２２から、ユーザ２０の個人関連情報であるＰＭＤ（Personal Meta Data）を、インターネット２１を介して取得し、取得したＰＭＤをデータベースとして記憶するｐＢａｓｅ（Personal Information Base）２３が接続されている。ｐＢａｓｅ２３は、コンピュータで構成され、インターネット２１に接続される他の情報処理装置と通信する。なお、ｐＢａｓｅ２３には、ＰＫ２２（ユーザ２０）以外のＰＫ（ユーザ）のＰＭＤも複数記憶されている。

【００８２】

また、インターネット２１には、コンピュータなどにより構成され、それぞれ所定の処理を実行するサービスシステム２４－１乃至２４－３が接続されている。サービスシステム２４－１乃至２４－３は、インターネット２１を介して、ＰＫ２２またはｐＢａｓｅ２３からＰＭＤを取得し、取得したＰＭＤに基づいて、所定のプログラムを実行することにより、情報提供、買い物代金の決済などのサービスをユーザに提供する。

【００８３】

例えば、サービスシステム２４－１は、パーソナルコンピュータにＷｅｂページ、音楽情報など提供するコンテンツサーバとされ、サービスシステム２４－２は、クレジットカードによる決済などを行うクレジットカード処理サーバとされ、サービスシステム２４－３は、ユーザ２０に対して行われるコミュニケーションを制御するコミュニケーションサーバとされる。また、アクセスポイント２５も、ＰＫ２２との通信を行うサービスシステム２４－４に包含される。なお、これらを個々に区別する必要がない場合、まとめてサービスシステム２４と称する。

【００８４】

この例では、サービスシステム２４－１乃至２４－４が表示されているが、実際には、多数のサービスシステムが存在する。また、サービスシステム２４は、パーソナルコンピュータ、サーバなどに限られるものではなく、コンソール端末、または各種のコンシューマエレクトロニクス機器（ＣＥ機器）などにより構成されるようにしてもよい。さらに、サービスシステム２４は、インターネット２１に接続されるものに限られることはなく、通信機能を有するものであれば、どこに設置されていてもよい。なお、ＰＫ２２とサービスシステム２４は、インターネット２１を介さずに、直接通信することも可能である。

【００８５】
図２は、ＰＫ２２の構成例を示すブロック図である。CPU（Central Processing Unit）１０１は、ROM（Read Only Memory）１０２に記憶されているプログラム、または記憶部１０８からRAM（Random Access Memory）１０３にロードされたプログラムに従って各種の処理を実行する。RAM１０３にはまた、CPU１０１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【００８６】
CPU１０１、ROM１０２、およびRAM１０３は、バス１０４を介して相互に接続されている。このバス１０４にはまた、入出力インタフェース１０５も接続されている。

【００８７】
入出力インタフェース１０５には、スイッチまたはボタンなどよりなる入力部１０６、およびドットマトリックスディスプレイ、スピーカ、振動モータなどにより構成され、画像、音声、点字または振動などによりユーザに提示する情報を出力する出力部１０７が接続されている。さらに、入出力インタフェース１０５には、ハードディスク、またはEEPROM（Electrically Erasable and Programmable Read Only Memory）などにより構成される記憶部１０８、無線送受信装置などにより構成される通信部１０９が接続されている。なお、通信部１０９は、ＲＦ通信（電磁波通信）、準静電界通信、光通信など通信方法に応じて、複数設けられるようにしてもよい。

【００８８】
ＲＦ（Radio Frequency）通信は、IEEE８０２．１１ｂに代表される無線ＬＡＮなどの通信であり、この通信により、所定のアクセスポイント（ハブ）の周囲およそ数十メートルで通信することができる。準静電界通信は、人体近傍に、遠隔伝播せず閉域のみに成立する物理的性質（エバネッセント性）をもつ閉じた静電的な情報空間を形成する通信方式であり、この通信により、人体が微弱な静電気のアンテナとなり人体の周囲およそ数センチメートル、または数メートルの限られた空間で通信することが可能となる。これにより、例えば、ＰＫ２２を携帯したユーザが、歩行しながら、ＰＫ２２に通信させることができる。

【００８９】
勿論、通信部１０９は、イーサネット（登録商標）などに代表される有線の電気的通信または赤外線などの光通信を行うものとすることも可能である。

【００９０】
入出力インタフェース１０５には、必要に応じてドライブ１１０が接続され、ドライブ１１０には、本発明のプログラムが記録された記録媒体として、例えば、リムーバブルメディア１１１が装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部１０８にインストールされる。

【００９１】
図３は、ｐＢａｓｅ２３の構成例を示すブロック図である。その構成は、図２に示したＰＫ２２の構成と同様であり、図３のＣＰＵ１２１乃至リムーバブルメディア１３１は、図２のＣＰＵ１０１乃至リムーバブルメディア１１１に対応している。各部の機能は、図２の場合と同様であり、詳細な説明は省略するが、通信部１２９は、無線送受信装置の他、ＬＡＮカード、モデムなどの有線による通信装置により構成される。

【００９２】
また、サービスシステム２４も図３と同様の構成であり、同図を適用する。

【００９３】
図４は、ＰＫ２２の記憶部１０８に記憶されるソフトウェア６０の構成例を示すブロック図である。ソフトウェア６０には、ＰＫ２２に保存される個人情報であるＰＭＤをデータベースとして記憶するＰＭＤＢ６７、および通信部１０９を制御して通信を行う通信モジュール６１が含まれている。

【００９４】
また、ユーザによる、ＰＭＤに対するアクセスの許可の指定を受け付けるユーザ制御許

可入力モジュール６２、サービスシステム２４からアクセス要求があったＰＭＤについて、ユーザにアクセス可否を判断させるために、そのＰＭＤを提示する許可項目確認モジュールが含まれている。さらに、サービスシステム２４のなりすましを防止するなりすまし防止モジュール６３、必要に応じてＰＭＤの変更を行うＰＭＤ変更モジュール６５が含まれている。ＤＢアクセスモジュール６６は、ユーザ制御許可入力モジュール６２乃至ＰＭＤ変更モジュール６５の指令（要求）に基づいて、ＰＭＤＢ６７にアクセスし、ＰＭＤの読み出しまたは変更を行う。

【００９５】

ＰＭＤＢ６７は、複数のＰＭＤにより構成されるデータベースであり、各ＰＭＤは、各サービスシステム２４に対応した固有のＩＤであるサービスＩＤをキーとして、各情報がディレクトリ状に関連付けられている。サービスＩＤ１のディレクトリ（ＰＭＤ）には、アクセス許可情報、メタデータＡ－１、メタデータＡ－２、メタデータＡ－３、・・・が関連付けられている。

【００９６】

アクセス許可情報は、そのディレクトリに関連付けられた情報に対する、サービスシステム２４からのアクセスの可否を表す情報であり、ユーザにより設定される。メタデータＡ－１、メタデータＡ－２、およびメタデータＡ－３、・・・は、サービスＩＤ１に対応するサービスシステム２４において、利用される個人関連情報であり、例えば、サービスＩＤ１に対応するサービスシステムが、映画やテレビ番組などのコンテンツを提供するコンテンツサーバである場合、メタデータＡ－１、メタデータＡ－２、およびメタデータＡ－３、・・・には、それぞれ視聴された番組のメタデータが記憶される。その他、ＰＭＤには、ＰＫ２２（ユーザ２０）を特定するユーザＩＤ、なりすまし防止処理において必要となる合言葉または暗号鍵などの認証情報、視聴された番組に基づくユーザの嗜好情報、およびテレビジョン受像機などを制御する制御情報などが記憶される。

【００９７】

同様にして、サービスＩＤ２のディレクトリにもアクセス許可情報、メタデータＢ－１、メタデータＢ－２、メタデータＢ－３、・・・が関連付けられている。そして、ＰＫが新たに、サービスシステム２４を利用する場合、新たなサービスＩＤが登録され、そのサービスＩＤに対応するディレクトリが生成される。そして、それぞれのディレクトリがＰＭＤとされ、ＰＭＤＢ６７が構成される。なお、ＰＭＤの詳細な構成例については、図２０を参照して後述する。

【００９８】

図５は、ＰＫ２２にサービスシステム２４に対応するサービスＩＤを、最初に登録（初期登録）するときの処理の流れを示すアローチャートである。ステップＳ１において、サービスシステム２４は、ＰＫ２２に対して、登録要求、サービスIDおよび、そのサービスシステムの読み出し変更対象となるメタデータを表す情報を送信し、ステップＳ２１において、ＰＫの通信モジュール６１により、これが受信される。

【００９９】

ステップＳ２２において、通信モジュール６１は、許可項目確認モジュール６３に受信内容を転送する。許可項目確認モジュール６３は、ステップＳ４２において、読み出し変更対象となるメタデータをユーザに提示する。このとき、例えば、メタデータの内容が、ドットマトリックスディスプレイ等に文字または図形等が表示されるか、スピーカを通じて音声により内容を読み上げられる。あるいはまた、メタデータの内容が、機械的機構により点字として生成され、提示されるか、振動によりモールス信号等の信号が生成され、提示されるようにしてもよい。

【０１００】

ステップＳ４３において、許可項目確認モジュール６３は、ユーザ制御許可入力モジュール６２に対して、確認要求を出力し、ステップＳ６１においてこれが取得される。ステップＳ６２において、ユーザ制御許可入力モジュール６２は、ステップＳ４２で提示された読み出し変更対象メタデータに対するアクセスを、ユーザが拒否したか否かを判定し、

拒否したと判定された場合、拒否信号を出力し、ステップＳ２３において、通信モジュール６１によりこれが受信される。ステップＳ２４において、通信モジュール６１は、拒否信号をサービスシステム２４に送信し、ステップＳ２でこれが受信される。

【０１０１】

一方、ステップＳ６２において、ステップＳ４２で提示された読み出し変更対象メタデータに対するアクセスを、ユーザが拒否していないと判定された場合、ユーザ制御許可入力モジュール６２は、ステップＳ６３において、ユーザの指定に基づいて、読み出し変更対象となるメタデータのそれぞれについて、例えば、「読み出しと変更を許可」、「読み出しのみ許可」などの情報を設定し、これらの情報がアクセス許可情報（図４）としてＰＭＤＢ６７に記憶される。ステップS６４において、ユーザ制御許可入力モジュール６２は、アクセス制御情報が設定されたことを、許可項目確認モジュール６３に対して通知し、ステップＳ４４において、これが取得される。ステップＳ４５において、許可項目確認モジュール６３は、なりすまし防止モジュール６４に対して、確認コードの生成要求を行い、ステップＳ８１において、なりすまし防止モジュール６４により、これが取得される。

【０１０２】

ステップＳ８２において、なりすまし防止モジュール６４は、確認コードを生成する。確認コードは、ＰＫ２２とサービスシステム２４が、次回通信を行うときのなりすまし防止方法を表すコードである。すなわち、不正なユーザ、または通信を盗聴した第３者などが、自身のアドレス、またはＩＤなどを詐称するなどして、ＰＫ２２、またはサービスシステム２４になりすましていないかを、互いに確認するための方法を表すコードである。

【０１０３】

ここで、なりすまし防止方法としては、例えば、合言葉による認証、公開鍵により暗号化された情報による認証、共通鍵により暗号化された情報による認証などが採用されるが、サービスシステム２４との通信において、どれだけの安全性が要求されるのか、どの程度、頻繁になりすまし防止のためのチェックをおこなうか、暗号鍵の管理方法の安全性と平易さ、暗号化と復号化における演算量、などを考慮して、そのサービスシステム２４との通信において、最適ななりすまし防止方法が選択され、そのなりすまし防止方法に対応する確認コードが生成される。なお、なりすまし防止の処理については、図６と図７を参照して後述する。

【０１０４】

ステップＳ８２において、なりすまし防止モジュール６４は、確認コードを、通信モジュール６１に対して出力し、ステップＳ２５において、通信モジュール６１によりこれが取得される。ステップＳ２６において、通信モジュール６１は、ステップＳ２５で取得された確認コードをサービスシステム２４に送信し、ステップＳ３においてこれが受信される。

【０１０５】

なお、このとき、ＰＫ２２（のユーザ）を特定するユーザＩＤも合わせてサービスシステム２４により受信され、サービスシステム２４は、ユーザＩＤと、そのユーザＩＤに対応する確認コードを記憶する。ユーザＩＤは、サービスシステム２４がＰＫ２２（のユーザ）を特定できるものであれば、どのような形式でもよい。例えば、ユーザＩＤが所定の数字の組み合わせにより構成されるようにしてもよいし、所定の文字列で構成されるようにしてもよい。また、複数のサービスシステム２４に対応して、それぞれ別のユーザＩＤが生成されるようにしてもよい。

【０１０６】

ステップＳ４６において、許可項目確認モジュール６３は、ＤＢアクセスモジュール６６に対して、サービスＩＤ登録要求を出力し、ステップＳ１０１において、ＤＢアクセスモジュール６６により、これが受信される。ステップＳ１０２において、ＤＢアクセスモジュール６６は、図９を参照して後述するサービスＩＤ登録処理を実行し、これによりサービスＩＤが登録され、サービスＩＤに対応するＰＭＤが生成される。

【０１０７】
このようにして、ＰＫ２２において、サービスシステム２４に対応するサービスＩＤが登録される。サービスＩＤが登録されるとき、そのサービスシステム２４により、読み出される、または変更されるＰＭＤのメタデータがユーザに提示されるようにしたので、ユーザは、より安心してサービスを受けることができる。また、ＰＫ２２が、そのサービスＩＤが登録されたサービスシステム２４と次回に通信するときは、確認コードに基づいて、なりすまし防止処理を行うことができる。同様に、サービスシステム２４が、そのユーザＩＤが登録されたＰＫ２２と次回に通信するときは、確認コードに基づいて、なりすまし防止処理を行うことができる。

【０１０８】
次に、図６と図７を参照して、ＰＫ２２が、既にサービスＩＤが登録されているサービスシステム２４との通信を行うときのなりすまし防止の処理について説明する。

【０１０９】
図６は、ＰＫ２２とサービスシステム２４の間のなりすまし防止方法として、合言葉による認証が採用されている場合のなりすまし防止の処理の流れを説明するアローチャートである。この例では、ＰＫ２２において、サービスシステム２４がなりすましではないことを確認し、その後サービスシステム２４において、ＰＫ２２がなりすましではないことを確認する。そして、ＰＫ２２とサービスシステム２４において、それぞれがなりすましではないことが確認できた後、ＰＭＤの読み出し、または変更の処理を行う。

【０１１０】
合言葉は、所定の文字列またはコードなどであり、ＰＫ２２において、サービスＩＤの登録時に、サービスＩＤに対応する合言葉として、サービスシステム２４を認証するための合言葉（サービス合言葉）とＰＫを認証するための合言葉（ＰＫ合言葉）が生成され、ＰＭＤＢ６７に記憶されている。また、サービスＩＤ登録時にサービス合言葉とＰＫ合言葉が、サービスシステム２４にも送信され、サービスシステム２４の記憶部１２８の中のデータベースに、サービス合言葉とＰＫ合言葉が、ＰＫ２２のユーザＩＤと関連付けられて記憶されている。

【０１１１】
ステップＳ２０１において、サービスシステム２４は、接続要求、サービスID、合言葉をＰＫ２２に送信し、ステップＳ２２１において、ＰＫ２２の通信モジュールによりこれが受信される。なお、ステップＳ２０１においては、上述したサービス合言葉が送信される。ステップＳ２２２において、通信モジュール６１は、ステップＳ２２１で受信した内容をなりすまし防止モジュール６４に転送し、ステップＳ２８１においてこれが受信される。

【０１１２】
ステップＳ２８２において、なりすまし防止モジュール６４は、図９を参照して後述するサービスＩＤマッチング処理を実行し、サービスＩＤの認識を行い、ステップＳ２８３において、ＤＢアクセスモジュール６６に対して、サービスＩＤに対応するユーザＩＤと合言葉の要求を通知し、ステップＳ３０１において、ＤＢアクセスモジュール６６によりこれが取得される。なお、ステップＳ２８２のサービスマッチング処理はＤＢアクセスモジュール６６で行われるようにしてもよい。

【０１１３】
ステップＳ３０２においてＤＢアクセスモジュール６６は、ＰＭＤＢ６７からサービスＩＤに対応するサービス合言葉、ＰＫ合言葉、およびユーザＩＤを読み出し、なりすまし防止モジュール６４に出力する。なりすまし防止モジュール６４は、ステップＳ２８４で取得されたサービス合言葉と、ステップＳ２８１で取得された合言葉を比較し、合言葉が一致しないと判定された場合、サービスシステム２４が、なりすましである可能性があると判定し、通信モジュール６１に対して、通信の拒否を表す拒否信号を通知し、ステップＳ２２３において、通信モジュール６１により、これが取得される。ステップＳ２２４において、通信モジュール６１は、拒否信号をサービスシステム２４に送信し、ステップＳ

２０２において、サービスシステム２４により、これが受信される。

【０１１４】

このように、通信を開始するとき、サービスシステム２４からサービスＩＤに対応する合言葉が送信されなかった場合、ＰＫ２２により、その通信は拒否される。

【０１１５】

一方、ステップＳ２８５において、サービス合言葉が一致すると判定された場合、なりすまし防止モジュール６４は、ステップＳ２８６において、サービスシステム２４が、なりすましでないことが確認できたことを表すコード（ＯＫ）と、ユーザＩＤ、ステップＳ２８４で取得されたＰＫ合言葉を、通信モジュール６１に出力し、ステップＳ２２５において、通信モジュール６１により、これが取得される。ステップＳ２２６において、通信モジュール６１は、ステップＳ２２５で取得された情報を、サービスシステム２４に送信し、ステップＳ２０３において、サービスシステム２４によりこれが受信される。

【０１１６】

ステップＳ２０４において、サービスシステム２４は、ステップＳ２０３で受信されたユーザＩＤに対応するＰＫ合言葉を、自身のデータベースから読み出し、ステップＳ２０３で受信された合言葉と比較し、合言葉が一致しているか否かを判定する。ステップＳ２０４において、合言葉が一致しないと判定された場合、ＰＫ２２が、なりすましである可能性があると判定し、サービスシステム２４は、通信の拒否を表す拒否信号をＰＫ２２に送信する。ＰＫ２２では、通信モジュール６１を介して、なりすまし防止モジュール６４によりステップＳ２８７で、これが受信される。

【０１１７】

このように、通信を開始するとき、ＰＫ２２からユーザＩＤに対応する合言葉が送信されなかった場合、サービスシステム２４により、その通信は拒否される。

【０１１８】

一方、ステップＳ２０４において、合言葉が一致すると判定された場合、サービスシステム２４は、ＰＫ２２がなりすましでないことが確認できたと判定し、ステップＳ２０５において、ＰＫ２２に対してＰＭＤの読み出し要求を送信し、ステップＳ２２７において、ＰＫ２２の通信モジュール６１により、これが受信される。ステップＳ２２８において、通信モジュール６１は、ステップＳ２２７で受信された内容を、ＤＢアクセスモジュール６６に対して出力し、ステップＳ３０３において、ＤＢアクセスモジュール６６により、これが取得される。

【０１１９】

ステップS３０４において、ＤＢアクセスモジュール６６は、サービスシステム２４から読み出し要求のあったＰＭＤ（のメタデータ）が、サービスシステム２４に対応するサービスＩＤに対して、読み出しが許可されているＰＭＤであるか否かを確認し、読み出しが許可されているＰＭＤである場合、そのＰＭＤをＰＭＤＢ６７から読み出す。そして、ステップＳ３０５において、ＤＢアクセスモジュール６６は、読み出したＰＭＤを通信モジュール６１に対して出力し、ステップＳ２２９において、通信モジュール６１により、これが取得される。

【０１２０】

ステップＳ２３０において、通信モジュール６１は、ステップＳ２２９で取得された情報を、サービスシステム２４に対して送信し、ステップＳ２０６において、サービスシステム２４により、これが受信される。

【０１２１】

ステップＳ２０７において、サービスシステム２４は、ステップＳ２０６で取得されたＰＭＤに基づいて、各種の処理（サービス対応処理）を実行する。ステップＳ２０７の処理の結果、ＰＭＤの変更が必要となる場合、サービスシステム２４は、ステップＳ２０８において、ＰＭＤの内容を変更し、ＰＫ２２に対して送信し、ステップＳ２３１において、ＰＫ２２の通信モジュール６１により、これが受信される。

【０１２２】

ステップＳ２３２において、通信モジュール６１は、ステップＳ２３１で受信された情報をＤＢアクセスモジュール６６に対して出力し、ステップＳ３０６においてＤＢアクセスモジュール６６によりこれが取得される。そして、ステップS３０７において、ＤＢアクセスモジュール６６は、ステップＳ３０６で取得されたＰＭＤが、サービスシステム２４に対応するサービスIDに対して変更許可のあるＰＭＤであるか否かを確認し、変更許可のあるＰＭＤである場合、ＰＭＤＢ６７の中の対応するＰＭＤの変更を行う（変更内容に対応して更新する）。

【０１２３】

このようにすることで、ＰＭＤの読み出し、または変更を行う前に、なりすましの確認することができるので、安全なサービスを提供することができる。さらに、ＰＫ２２によるサービスシステム２４のなりすましの確認と、サービスシステム２４によるＰＫ２２のなりすましの確認が行われるようにしたので、より安全なサービスを提供することができる。

【０１２４】

次に図７を参照して、ＰＫ２２が、既にサービスＩＤが登録されているサービスシステム２４との通信を行うときのなりすまし防止の処理の別の例について説明する。図７は、ＰＫ２２とサービスシステム２４の間のなりすまし防止方法として、公開鍵により暗号化された情報による認証が採用されている場合のなりすまし防止の処理の流れを説明するアローチャートである。

【０１２５】

この例においても、ＰＫ２２において、サービスシステム２４がなりすましではないことを確認し、その後サービスシステム２４において、ＰＫ２２がなりすましではないことを確認する。そして、ＰＫ２２とサービスシステム２４において、それぞれがなりすましではないことが確認できた後、ＰＭＤの読み出し、または変更の処理を行う。

【０１２６】

また、この例においては、ＰＫ２２とサービスシステム２４は、RSAなどの公開鍵方式の暗号アルゴリズムによる情報の暗号化または複合化の処理を実行する機能を有しており、サービスＩＤを登録するとき、ＰＫ２２により、サービスシステム２４の公開鍵が、サービスシステム２４のサービスＩＤに関連付けられてＰＭＤＢ６７に記憶されており、サービスシステム２４により、ＰＫ２２の公開鍵が、ＰＫ２２のユーザＩＤに関連づけられて記憶部１２８の中のデータベースに記憶されている。ＰＫ２２とサービスシステム２４の秘密鍵は、それぞれの記憶部１０８または１２８に記憶されている。

【０１２７】

ステップＳ４０１において、サービスシステム２４は、接続要求とサービスＩＤをＰＫ２２に送信し、ステップＳ４２１において、ＰＫ２２の通信モジュールによりこれが受信される。ステップＳ４２２において、通信モジュール６１は、ステップＳ４２１で受信した情報をなりすまし防止モジュール６４に転送し、ステップＳ４８１においてこれが受信される。

【０１２８】

ステップＳ４８２において、なりすまし防止モジュール６４は、図１０を参照して後述するサービスＩＤマッチング処理を実行し、サービスＩＤの認識を行い、ステップＳ４８３において、ＤＢアクセスモジュール６６に対して、サービスＩＤに対応するユーザＩＤ、ＰＫの秘密鍵、およびサービスシステム２４の公開鍵の要求を通知し、ステップＳ５０１において、ＤＢアクセスモジュール６６によりこれが取得される。なお、ステップＳ４８２のサービスマッチング処理は、ＤＢアクセスモジュール６６において実行されるようにしてもよい。

【０１２９】

ステップＳ５０２において、ＤＢアクセスモジュール６６は、サービスＩＤに対応するサービスシステム２４の公開鍵と、ＰＫの秘密鍵をＰＭＤＢ６７から読み出し、なりすまし防止モジュール６４に対して出力し、ステップＳ４８４において、なりすまし防止モジ

ュール６４により、これが取得される。

【０１３０】

ステップＳ４８５において、なりすまし防止モジュール６４は、サービスシステム２４を認証するため、所定のコードで構成されるチャンレンジコードを生成し、チャレンジコードをサービスＩＤに対応する公開鍵（サービスシステム２４の公開鍵）で暗号化し、暗号化されたチャレンジコードとユーザＩＤを通信モジュール６１に対して出力し、ステップＳ４２３において、通信モジュール６１により、これが取得される。ステップＳ４２４において、通信モジュール６１は、ステップＳ４２３で取得された情報をサービスシステム２４に送信し、ステップＳ４０２において、サービスシステム２４により、これが受信される。

【０１３１】

ステップＳ４０３において、サービスシステム２４は、ステップＳ４０２で受信された、暗号化されたチャレンジコードをサービスシステム２４の秘密鍵により復号し、復号されたチャレンジコードをレスポンスコードとし、レスポンスコードをユーザＩＤに対応する公開鍵（ＰＫ２２の公開鍵）で暗号化してＰＫ２２に対して送信し、ステップＳ４２５において、ＰＫ２２の通信モジュール６１により、これが受信される。

【０１３２】

ステップＳ４２６において、通信モジュール６１は、ステップＳ４２５で受信された、暗号化されたレスポンスコードを、なりすまし防止モジュール６４に対して出力し、ステップＳ４８６において、なりすまし防止モジュール６４により、これが取得される。

【０１３３】

ステップＳ４８７において、なりすまし防止モジュール６４は、ステップＳ４８６で取得された、暗号化されたレスポンスコードをＰＫ２２の秘密鍵で複合化し、ステップＳ４８５で生成したチャレンジコードと比較して、チャレンジコードとレスポンスコードが一致しているか否かを判定し、チャレンジコードとレスポンスコードが一致しないと判定された場合、サービスシステム２４が、なりすましである可能性があると判定し、通信モジュール６１に対して、通信の拒否を表す拒否信号を通知し、ステップＳ４２６において、通信モジュール６１により、これが取得される。ステップＳ４２７において、通信モジュール６１は、拒否信号をサービスシステム２４に送信し、ステップＳ４０４において、サービスシステム２４により、これが受信される。

【０１３４】

このように、通信を開始するとき、ＰＫ２２からチャレンジコードが送信され、サービスシステム２４からチャレンジコードと一致するレスポンスコードが返信されなかった場合、ＰＫ２２により、その通信は拒否される。

【０１３５】

一方、ステップＳ４８７において、チャレンジコードとレスポンスコードが一致すると判定された場合、なりすまし防止モジュール６４は、ステップＳ４８８において、サービスシステム２４がなりすましでないことが確認できたことを表すコード（ＯＫ）を、通信モジュール６１を介して、サービスシステム２４に送信し、ステップＳ４０５において、サービスシステム２４によりこれが受信される。

【０１３６】

ステップＳ４０６において、サービスシステム２４は、ＰＫ２２を認証するため、所定のコードにより構成されるチャレンジコードを生成し、チャレンジコードをユーザＩＤに対応する公開鍵（ＰＫ２２の公開鍵）で暗号化し、暗号化されたチャレンジコードをＰＫ２２に対して送信し、ステップＳ４２９において、ＰＫ２２の通信モジュール６１によりこれが受信される。ステップＳ４３０において、通信モジュール６１は、ステップＳ４２９で受信された情報をなりすまし防止モジュール６４に対して出力し、ステップＳ４８９において、なりすまし防止モジュール６４により、これが取得される。

【０１３７】

ステップＳ４９０において、なりすまし防止モジュール６４は、ステップＳ４８９で受

信された、暗号化されたチャレンジコードをＰＫ２２の秘密鍵で復号し、復号されたチャレンジコードをレスポンスコードとし、レスポンスコードをサービスＩＤに対応する公開鍵（サービスシステム２４の公開鍵）で暗号化し、通信モジュール６１に対して出力し、ステップＳ４３１において、通信モジュール６１により、これが取得される。ステップＳ４３２において、通信モジュール６１は、ステップＳ４３１で取得された情報をサービスシステム２４に対して送信し、ステップＳ４０７において、サービスシステム２４によりこれが受信される。

【０１３８】

ステップＳ４０８において、サービスシステム２４は、ステップＳ４０７で受信された、暗号化されたレスポンスコードを、サービスシステム２４の秘密鍵で復号し、復号されたレスポンスコードが、ステップＳ４０６で生成されたチャレンジコードと一致するか否かを判定し、チャレンジコードとレスポンスコードが一致しないと判定された場合、ＰＫ２２が、なりすましである可能性があると判定し、ＰＫ２２に対して、通信の拒否を表す拒否信号を送信し、ステップＳ４３３で、ＰＫ２２の通信モジュール６１により、これが受信される。ステップＳ４３４において、通信モジュール６１は、ステップＳ４３３で受信された情報を、なりすまし防止モジュール６４に対して送信し、ステップＳ４９１において、なりすまし防止モジュール６４により、これが取得される。

【０１３９】

このように、通信を開始するとき、サービスシステム２４からチャレンジコードが送信され、ＰＫ２２からチャレンジコードと一致するレスポンスコードが返信されなかった場合、サービスシステム２４により、その通信は拒否される。

【０１４０】

一方、ステップＳ４０８において、チャレンジコードとレスポンスコードが一致すると判定された場合、サービスシステム２４は、ＰＫ２２がなりすましでないことが確認できたと判定し、ステップＳ４０９において、ＰＫ２２に対してＰＭＤの読み出し要求を送信し、ステップＳ４３５において、ＰＫ２２の通信モジュール６１により、これが受信される。ステップＳ４３６において、通信モジュール６１は、ステップＳ４３５で受信された情報を、ＤＢアクセスモジュール６６に対して出力し、ステップＳ５０３において、ＤＢアクセスモジュール６６により、これが取得される。

【０１４１】

ステップS５０４において、ＤＢアクセスモジュール６６は、サービスシステム２４から読み出し要求のあったＰＭＤ（のメタデータ）が、サービスシステム２４に対応するサービスＩＤに対して、読み出しが許可されているＰＭＤであるか否かを確認し、読み出しが許可されているＰＭＤである場合、そのＰＭＤをＰＭＤＢ６７から読み出す。そして、ステップＳ５０５において、ＤＢアクセスモジュール６６は、読み出したＰＭＤを通信モジュール６１に対して出力し、ステップＳ４３７において、通信モジュール６１により、これが取得される。

【０１４２】

ステップＳ４３８において、通信モジュール６１は、ステップＳ４３７で取得された情報を、サービスシステム２４に対して送信し、ステップＳ４１０において、サービスシステム２４により、これが受信される。

【０１４３】

ステップＳ４１１において、サービスシステム２４は、ステップＳ４１０で取得されたＰＭＤに基づいて、各種の処理（サービス対応処理）を実行する。ステップＳ４１１の処理の結果、ＰＭＤの変更が必要となる場合、サービスシステム２４は、ステップＳ４１２において、ＰＭＤの内容を変更し、ＰＫ２２に対して送信し、ステップＳ４３９において、ＰＫ２２の通信モジュール６１により、これが受信される。

【０１４４】

ステップＳ４４０において、通信モジュール６１は、ステップＳ４３９で受信された情報をＤＢアクセスモジュール６６に対して出力し、ステップＳ５０６においてＤＢアクセ

スモジュール６６によりこれが取得される。そして、ステップＳ５０７において、ＤＢアクセスモジュール６６は、ステップＳ５０６において取得されたＰＭＤが、サービスシステム２４に対応するサービスＩＤに対して変更許可のあるＰＭＤであるか否かを確認し、変更許可のあるＰＭＤである場合、ＰＭＤＢ６７の中の対応するＰＭＤの変更を行う（変更内容に更新する）。

【０１４５】

このようにすることで、ＰＭＤの読み出し、または変更を行う前に、ＰＫ２２とサービスシステム２４が、互いになりすましでないことを確認することができるので、安全なサービスを提供することができる。また、ＰＫ２２またはサービスシステム２４を認証するためのチャレンジコードとレスポンスコードは、それぞれＰＫ２２とサービスシステム２４の公開鍵と秘密鍵により、暗号化または復号化されるので、仮に、第三者に通信が傍受されても、チャレンジコードとレスポンスコードの内容は、秘匿されるので、より確実になりすましを防止することができる。

【０１４６】

なお、図７においては、公開鍵方式の暗号アルゴリズムにより、チャレンジコードとレスポンスコードを暗号化する例について説明したが、ＰＫ２２とサービスシステム２４が、公開鍵方式の暗号アルゴリズムではなく、共通鍵方式の暗号アルゴリズムで、情報の暗号化または複合化の処理を実行する機能を有し、ＰＫ２２とサービスシステム２４において、互いに共通の暗号鍵が保持され、チャレンジコードとレスポンスコードが、その鍵で暗号されることにより通信が行われるようにしてもよい。

【０１４７】

この場合、サービスＩＤの登録を行うとき、ＰＫ２２により、そのサービスＩＤに対応する暗号鍵が生成され、サービスＩＤに関連付けられてＰＭＤＢ６７に記憶されると同時に、同じ暗号鍵が、サービスシステム２４に送信され、ＰＫ２２のユーザＩＤに対応付けられてサービスシステム２４のデータベースに記憶される。

【０１４８】

暗号鍵が漏洩した場合、ＰＫ２２とサービスシステム２４は、暗号鍵を変更する必要がある。例えば、あるサービスシステムの公開鍵方式の暗号アルゴリズムで用いられる秘密鍵が漏洩した場合、そのサービスシステムを利用する多数のＰＫにおいて、サービスＩＤに対応する公開鍵を変更する必要がある。しかし、ＰＫ２２とサービスシステム２４において、互いに共通の暗号鍵が保持されるようにすれば、暗号鍵が漏洩した場合でも、その鍵を使うＰＫ２２とサービスシステム２４の暗号鍵のみ変更するだけで、対処することができる。

【０１４９】

なお、図７においては、チャレンジコードとレスポンスコードが暗号化される例について説明したが、通信内容の全てが暗号化されるようにしてもよい。

【０１５０】

また、図７の例では、秘密鍵（または共通鍵）がＰＫ２２の中（ＰＭＤＢ６７）に保管される例について説明したが、ＰＫ２２とは異なる機器、例えば、図１のＳＢ２６に保管されるようにしてもよい。この場合、サービスシステム２４と通信を行うに先立って、ＰＫ２２とＳＢ２６が通信を行い、ＳＢ２６からＰＫ２２に秘密鍵が送信される（このとき、ＳＢはＰＫに対して、１つのサービスシステムとして通信する）。ＰＫは、一定時間経過すると秘密鍵を消去する処理を行い、必要なときには、都度、ＳＢ２６と通信して秘密鍵を取得する。

【０１５１】

この場合のＰＫ２２の鍵管理処理について、図８を参照して説明する。この処理は、ＰＫ２２が、サービスシステム２４との通信を行うとき、図７に示されるようななりすまし防止の処理が行われるのに先立って実行される。

【０１５２】

ステップＳ６８１において、ＰＫ２２のＣＰＵ１０１は、ＳＢ２６から鍵を取得し、記

憶部１０８に記憶する。ステップＳ６８２において、ＣＰＵ１０１は、所定の時間（例えば、１時間）が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。ステップＳ６８２において、所定の時間が経過したと判定された場合、ステップＳ６８３において、記憶部１０８に記憶されている鍵を消去する。

【０１５３】

このようにして、鍵の管理が行われる。このようにすることで、例えば、ＰＫ２２が盗まれた場合でも、秘密鍵が漏洩することを防止することができる。

【０１５４】

次に、図９を参照して、図５のステップＳ１０２のサービスＩＤ登録処理の詳細について説明する。多くの場合、サービスシステム２４は、インターネット２１に接続されたサーバである。この処理は、図５のステップＳ１０２において、サービスシステム２４を特定する情報として、サービスシステム２４を構成するサーバのURI（Uniform Resource Identifiers）が取得された場合、実行される。

【０１５５】

ステップＳ８０１において、ＤＢアクセスモジュール６６は、URIを取得する。ステップＳ８０２において、ＤＢアクセスモジュール６６は、マスクがあるか否かを判定する。マスクは、URIの中の所定のセグメントを示す情報であり、例えば、ユーザにより、予め設定されている。

【０１５６】

URIは、インターネット２１でのユニークなアドレスとして管理されており、全世界でのさまざまなサーバに、例えば、「http://aaa.bbb.ccc」のようなネーミングが行われている。ここで、「http://aaa.bbb.」（または「http://aaa.」）の部分は、通常そのサーバが提供するサービスに対応する会社名などを示し、cccの部分は、そのサービスの内容に応じて変化する。例えば、ユーザが、特定の会社が行うさまざまなサービスすべてに対して、ＰＭＤの読み出しまたは変更を許可する場合、「http://aaa.bbb.」の部分のみを参照してサービスシステム２４を特定すればよい。このような場合、マスクとして、下位１セグメント（「ccc」の部分）が設定される。

【０１５７】

ステップＳ８０２において、マスクがあると判定された場合、ステップＳ８０４に進み、ＤＢアクセスモジュール６６は、サービスＩＤとして、マスクされた部分を取り除いたURI（「http://aaa.bbb.」の部分）を登録する。ステップＳ８０２において、マスクがないと判定された場合、ステップＳ８０３に進み、ＤＢアクセスモジュール６６は、サービスＩＤとしてURIをそのまま（「http://aaa.bbb.ccc」）登録する。

【０１５８】

ステップＳ８０３またはＳ８０４の処理の後、ステップＳ８０５に進み、ＤＢアクセスモジュール６６は、サービスＩＤと、そのサービスＩＤに対応するサービスシステム２４において、利用される個人関連情報を関連づけて、そのサービスＩＤに対応するＰＭＤを生成する。

【０１５９】

このようにして、サービスＩＤが登録される。

【０１６０】

次に、図１０を参照して、図６のステップＳ２８２、または図７のステップＳ４８２のサービスＩＤマッチング処理の詳細について説明する。なお、この例では、サービスＩＤマッチング処理が、ＤＢアクセスモジュール６６により実行されるものとする。

【０１６１】

ステップＳ８４１において、ＤＢアクセスモジュール６６は、URIを取得する。ステップＳ８４２において、ＤＢアクセスモジュール６６は、URIをサービスＩＤと同じ長さに切り出す。このとき、例えば、URIとして「http://aaa.bbb.ccc」が取得された場合、「http://aaa.bbb.」の部分が切り出される。ステップＳ８４３において、ＤＢアクセスモジュール６６は、ステップＳ８４２で切り出されたURIを登録されたサービスＩＤと比較す

る。

【０１６２】

ステップＳ８４４において、ＤＢアクセスモジュール６６は、ステップＳ８４３における比較の結果、サービスＩＤと一致したか否かを判定し、一致しないと判定された場合、ステップＳ８４６に進み、登録されたサービスＩＤを全てチェックしたか否かを判定し、まだ、全てチェックしていないと判定された場合、ステップＳ８４７に進み、ステップＳ８４２で切り出されたURIを次のサービスＩＤと比較し、ステップＳ８４４に戻る。

【０１６３】

ステップＳ８４４において、ステップＳ８４３における比較の結果、サービスＩＤと一致したと判定された場合、ステップＳ８４５に進み、一致したサービスＩＤを、サービスシステム２４を特定するサービスＩＤとして認識する。

【０１６４】

ステップＳ８４６において、登録されたサービスＩＤを全てチェックしたと判定された場合、ステップＳ８４８に進みＤＢアクセスモジュール６６は、このサービスの拒否を通知する。

【０１６５】

このようにして、サービスＩＤの認識が行われる。

【０１６６】

ところで、上述したようにＰＫ２２には、ＰＭＤとして個人関連情報が記憶されており、仮にＰＫ２２を盗まれても、悪用されないように、ＰＫ２２の内部に保存されたＰＭＤが暗号化されて秘匿されることが好ましい。

【０１６７】

例えば、ＰＭＤをＰＫ２２の公開鍵で暗号化しておいて、必要に応じて秘密鍵を用いて復号するようにしてもよい。秘密鍵は、ＳＢに保管されているので、ＰＫ２２とＳＢの通信が途絶えた場合には、ＰＫの中に秘密鍵がないことになり、ＰＭＤを読み出したり変更したりすることができない。

【０１６８】

あるいはまた、ＰＫ２２が、ユーザ２０を認証し、正当なユーザ２０であると確認された場合だけ、ＰＭＤが利用可能とされるようにしてもよい。

【０１６９】

例えば、一定の時間内に、ワンタイムパスワード（固定パスワードでもよい）または後述する生体認証により、そのユーザが正当なユーザであることが確認できない場合、ＰＭＤの読み出しまたは変更の制御が禁止されるようにしてもよいし、ＰＭＤが自動的に消去されるようにしてもよい。ＰＭＤが消去された場合、ワンタイムパスワードまたは生体認証により、正当なユーザであることが確認されたとき、ｐＢａｓｅ２３に保存されているＰＭＤを利用して、ＰＫ２２のＰＭＤが回復される。

【０１７０】

図１１は、ＰＫ２２によるユーザ２０の認証方法の例を示す図である。図１１Ａは、ＰＫ２２は、ユーザ２０が常に携帯するチップ２０１を検知してユーザの認証を行う例を示す図である。チップ２０１は、例えば、特定の周波数の電波を常に発信する充分に小さい発信機であり、ユーザ２０により常に携帯さている。この場合、ＰＫ２２には、チップ２０１が発信する電波を検知するセンサが設けられており、センサは、ＰＫ２２の入力部１０６に接続されているものとする。ＰＫ２２は、予め登録されたチップ２０１が発信する周波数の電波を検知することによりユーザ２０を認証する。

【０１７１】

この場合、ＰＫ２２がユーザ２０を認証するユーザ認証処理１について、図１２を参照して説明する。この処理は、例えば、ＰＫ２２の電源がＯＮの状態である間、常に継続して実行される。

【０１７２】

ステップＳ９０１において、ＰＫ２２のＣＰＵ１０１は、センサにより検知された信号

を登録されているチップ２０１の信号と比較する。ステップＳ９０２において、ＣＰＵ１０１は、ステップＳ９０１の比較の結果、信号が一致したか否かを判定し、一致しないと判定された場合、ステップＳ９０１に戻る。

【０１７３】

ステップＳ９０２において、信号が一致したと判定された場合、ステップＳ９０３に進み、ユーザ認証情報を記憶する。このとき、ユーザ２０を認証したことを表す情報が、現在時刻（日時）とともに、ユーザ認証情報として、記憶部１０８に記憶される。

【０１７４】

ステップＳ９０４において、ＣＰＵ１０１は、所定の時間（例えば、１時間）が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。ステップＳ９０４において、所定の時間が経過したと判定された場合、ステップＳ９０５に進み、ＣＰＵ１０１は、ユーザ認証情報を削除する。その後、処理は、ステップＳ９０１に戻り、それ以降の処理が繰り返し実行される。

【０１７５】

あるいはまた、ユーザの生体的特徴（指紋、声紋、虹彩、歩紋等）を用いた認証、すなわち生体認証が行われるようにしてもよい。図１１Ｂは、ユーザ２０の生体的特徴としての歩紋２０２を検知することで、ユーザ２０を認証する例を示す図である。この場合、ＰＫ２２には、準静電界の変化を検知するセンサが設けられており、センサは、ＰＫ２２の入力部１０６に接続されているものとする。ＰＫ２２は、予め登録されたユーザ２０の歩紋を検知することによりユーザ２０を認証する。なお、歩紋とは、人が歩行するとき、人体に発生する準静電界の変化パターンであり、このパターンを用いて人を認識することができる（例えば、特開２００３－５８８５７　歩行検出方法、歩行検出装置　参照）。

【０１７６】

この場合、ＰＫ２２がユーザ２０を認証するユーザ認証処理２について、図１３を参照して説明する。この処理は、例えば、ＰＫ２２の電源がＯＮの状態である間、常に継続して実行される。

【０１７７】

ステップＳ９２１において、ＰＫ２２のＣＰＵ１０１は、センサにより検知された準静電界の変化パターン（歩紋）を登録されているユーザ２０の歩紋と比較する。ステップＳ９０２において、ＣＰＵ１０１は、ステップＳ９２１の比較の結果、歩紋が一致したか否かを判定し、一致しないと判定された場合、ステップＳ９２１に戻る。

【０１７８】

ステップＳ９２２において、歩紋が一致したと判定された場合、ステップＳ９２３に進み、ユーザ認証情報を記憶する。このとき、ユーザ２０を認証したことを表す情報が、現在時刻（日時）とともに、ユーザ認証情報として、記憶部１０８に記憶される。

【０１７９】

ステップＳ９２４において、ＣＰＵ１０１は、所定の時間（例えば、１時間）が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。ステップＳ９２４において、所定の時間が経過したと判定された場合、ステップＳ９２５に進み、ＣＰＵ１０１は、ユーザ認証情報を削除する。その後、処理は、ステップＳ９２１に戻り、それ以降の処理が繰り返し実行される。

【０１８０】

このようにして、所定の時間毎に、ＰＫ２２によりユーザ２０が認証される。以上においては、チップ２０１または歩紋２０２によりユーザ２０が認証される例について説明したが、ユーザの認証方法は、これに限られるものではない。例えば、ＰＫ２２を、近傍のパーソナルコンピュータと通信させ、パーソナルコンピュータから入力されるパスワードに基づいて、ユーザが認証されるようにしてもよい。

【０１８１】

また、上述したように、ＰＫ２２においては、ユーザが正当なユーザであることが確認（認証）できない場合、ＰＭＤが自動的に消去されるようにすることができる。この場合

のＰＭＤ管理処理について、図１４を参照して説明する。この処理は、ＰＫ２２において、ＰＭＤが必要となる都度、実行される。なお、実行に先立って、ＰＫ２２のＣＰＵ１０１により、図１２のステップＳ９０３、または図１３のステップＳ９２３で記憶されたユーザ認証情報が、記憶部１０８の中に存在する（ユーザが認証されている）ことが確認される。

【０１８２】

ステップＳ９４１において、ＣＰＵ１０１は、ｐＢａｓｅ２３と通信し、ｐＢａｓｅ２３からＰＭＤを取得し、記憶部１０８に記憶する。ステップＳ９４２においてＣＰＵ１０１は、ステップＳ９４１で、ＰＭＤを取得してから所定の時間（例えば、３時間）が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。

【０１８３】

ステップＳ９４２において、所定の時間が経過したと判定された場合、ステップＳ９４３に進み、ＣＰＵ１０１は、ユーザが認証されたか否かを判定する。このとき、図１２のステップＳ９０３、または図１３のステップＳ９２３で記憶されたユーザ認証情報が、記憶部１０８の中に存在するか否かが判定され、ユーザ認証情報が存在する場合、ユーザが認証されたと判定され、ユーザ認証情報が存在しない場合、ユーザが認証されなかったと判定される。ステップＳ９４３において、ユーザが認証されたと判定された場合、処理はステップＳ９４２に戻り、それ以降の処理が繰り返し実行される。

【０１８４】

ステップＳ９４３において、ユーザが認証されなかったと判定された場合、ＣＰＵ１０１は、ステップＳ９４４に進み、ステップＳ９４１で取得したＰＭＤを記憶部１０８から消去する。

【０１８５】

このようにして、ＰＫ２２において、ユーザが正当なユーザであることが確認（認証）できない場合、ＰＭＤが自動的に消去される

【０１８６】

ところで、上述したように、ＰＫ２２は、ユーザが簡単に持ち運べる小型のコンピュータであり、ＰＫ２２に、いろいろなインタフェース（例えば、ディスプレイ、タッチパッドなど）を直接配置すると、ＰＫ２２の大きさが大きくなり、重量も重くなるので、ユーザが簡単に持ち運ぶことができなくなる恐れがある。

【０１８７】

このために、ＰＫ２２に直接配置されるインタフェースは、できるだけ小さくし、例えば、複雑な情報の入力または出力に用いられるインタフェースとして、ＰＫ２２の外部にある機器などを利用できることが望ましい。

【０１８８】

図１５は、ＰＫ２２が外部コンソール２２１と、外部コンソール２２２を入力または出力に用いられるインタフェースとして利用する例を示す図である。この場合、ＰＫ２２は、外部コンソール２２１および２２２と、ＲＦ通信などの無線通信を行う。外部コンソール２２１には、項目リスト画面２４２とプッシュスイッチ２４１が設けられており、例えば、項目リスト画面２４２にＰＭＤのリストが表示され、プッシュスイッチ２４１をユーザが操作することにより、項目リスト画面２４２に表示されたＰＭＤに対するアクセス許可が指定される。

【０１８９】

外部コンソール２２２には、タッチパット付ディスプレイ２６１が設けられており、タッチパッド付ディスプレイ２６１に表示される操作卓を変化させることができ、例えば、サービスＩＤに対応して異なるインタフェースが提供される。

【０１９０】

なお、外部コンソール２２１または２２２は、ＰＫ２２に対して、インタフェースサービスを提供する、サービスシステムの一つとみなすこともできる。この場合、ＰＫ２２は、外部コンソール２２１または２２２の制御コードを記憶するサーバをサービスシステム

として通信を行い、外部コンソール２２１または２２２の制御コードを取得する。その後、外部コンソール２２１または２２２をサービスシステムとして通信を行い、外部コンソール２２１または２２２に制御コードを実装させる。

【０１９１】

このように、サービスシステム２４から、ＰＫ２２を介して、外部コンソール２２１などの周辺機器を制御させることにより、図１６に示されるように、サービスシステム２４に対して、周辺機器（外部コンソール２２１など）のアドレスなどのアクセスキー２８０を隠蔽して、サービスの提供を受けることができる。

【０１９２】

次に、図１７を参照して、ＰＫ２２、ｐＢａｓｅ２３、およびサービスシステム２４によりＰＭＤが利用される様子を説明する。ＰＫ２２は、上述したように、ＲＦ通信、準静電界通信、光通信などの無線通信により、インターネット２１に接続されたアクセスポイント２５と通信し、インターネット２１に接続される。このとき、図１７Ａに示されるように、インターネット２１を介してＰＫ２２とｐＢａｓｅ２３が接続され、両者のＰＭＤの内容が比較され、ＰＭＤの同期が行われる。例えば、ＰＫ２２のＰＭＤの内容が更新されている場合、ｐＢａｓｅ２３のＰＭＤも同様に更新され、ＰＭＤの同期が行われる。なお、ＰＭＤの同期の詳細については後述する。

【０１９３】

また、例えば、ＰＫ２２に記憶しきれないＰＭＤをｐＢａｓｅ２３に記憶させ、図１７Ｂに示されるように、サービスシステム２４は、ｐＢａｓｅ２３のＰＭＤを参照し、ＰＫ２２のユーザに対するサービスを行うようにすることもできる。

【０１９４】

あるいはまた、ＰＫ２２をインターネット２１に接続できない場合、ｐＢａｓｅ２３には、ＰＫ２２のＰＭＤが記憶されているので、図１７Ｃに示されるように、ｐＢａｓｅ２３を、ＰＫ２２に代わってサービスシステム２４と通信させることにより（ＰＫ２２の代用としてｐＢａｓｅ２３を利用して）、ユーザはサービスの提供を受けることができる。このような場合、ＰＫ２２に代わったｐＢａｓｅ２３とサービスシステム２４の間でなりすまし防止の処理が行われ、ＰＭＤの送受信が行われる。

【０１９５】

図１８と図１９を参照して、図１７Ｃの場合の、ｐＢａｓｅ２３とサービスシステム２４との間の処理の流れを説明する。図１８の例では、ＰＫ２２（のユーザ）に対応するＰＭＤが、ｐＢａｓｅ２３の記憶部１２８の中のデータベースに記憶されているものとし、サービスシステム２４との間で、なりすまし防止方法として、図６の場合と同様に合言葉による認証が採用されているものとする。

【０１９６】

同図においては、ｐＢａｓｅ２３において、サービスシステム２４がなりすましではないことを確認し、その後サービスシステム２４において、ｐＢａｓｅ２３がなりすましではないことを確認する。そして、ｐＢａｓｅ２３とサービスシステム２４において、それぞれがなりすましではないことが確認できた後、ＰＭＤの読み出し、または変更の処理を行う。また、この例においては、ＰＫ合言葉、サービスシステム合言葉、ＰＫ２２のユーザＩＤ、およびサービスシステム２４のサービスＩＤは、やはりＰＫ２２のＰＭＤとして、ｐＢａｓｅ２３の記憶部１２８の中のデータベースに記憶されているものとする。

【０１９７】

ステップＳ１１０１において、サービスシステム２４は、接続要求、サービスID、合言葉をｐＢａｓｅ２３に送信し、ステップＳ１１２１において、これが受信される。ステップＳ１１２２において、ｐＢａｓｅ２３は、図１０を参照して上述したサービスＩＤマッチング処理を実行し、サービスＩＤの認識を行い、サービスＩＤに対応するサービス合言葉、ＰＫ合言葉、およびユーザＩＤを記憶部１２８のデータベースから読み出す。ステップＳ１１２３において、ｐＢａｓｅ２３は、ステップＳ１１２１で取得されたサービス合言葉と、記憶部１２８のデータベースから読み出されたサービス合言葉を比較し、サービ

ス合言葉が一致しないと判定された場合、サービスシステム２４が、なりすましである可能性があると判定し、サービスシステム２４に対して、通信の拒否を表す拒否信号を送信し、ステップＳ１１０２において、これが受信される。

【０１９８】

このように、通信を開始するとき、サービスシステム２４からサービスＩＤに対応する合言葉が送信されなかった場合、ｐＢａｓｅ２３により、その通信は拒否される。

【０１９９】

一方、ステップＳ１１２３において、サービス合言葉が一致すると判定された場合、ｐＢａｓｅ２３は、ステップＳ１１２４において、サービスシステム２４がなりすましでないことが確認できたことを表すコード（ＯＫ）と、ユーザＩＤ、およびユーザＩＤに対応するＰＫ合言葉を、サービスシステム２４に送信し、ステップＳ１１０３において、これが受信される。

【０２００】

ステップＳ１１０４において、サービスシステム２４は、ステップＳ１１０３で受信されたユーザＩＤに対応するＰＫ合言葉を、自身のデータベースから読み出し、ステップＳ１１０３で受信されたＰＫ合言葉と比較し、ＰＫ合言葉が一致しているか否かを判定する。ステップＳ１１０４において、ＰＫ合言葉が一致しないと判定された場合、ｐＢａｓｅ２３が、なりすましである可能性があると判定し、サービスシステム２４は、通信の拒否を表す拒否信号をｐＢａｓｅ２３に送信し、ステップＳ１１２５で、これが受信される。

【０２０１】

このように、通信を開始するとき、ｐＢａｓｅ２３からユーザＩＤに対応する合言葉が送信されなかった場合、サービスシステム２４により、その通信は拒否される。

【０２０２】

一方、ステップＳ１１０４において、ＰＫ合言葉が一致すると判定された場合、サービスシステム２４は、ｐＢａｓｅ２３がなりすましでないことが確認できたと判定し、ステップＳ１１０５において、ｐＢａｓｅ２３に対してＰＭＤの読み出し要求を送信し、ステップＳ１１２６において、これが受信される。ステップS１１２７において、ｐＢａｓｅ２３は、サービスシステム２４から読み出し要求のあったＰＭＤが、サービスシステム２４に対応するサービスＩＤに対して、読み出しが許可されているＰＭＤであるか否かを確認し、読み出しが許可されているＰＭＤである場合、そのＰＭＤを記憶部１２８のデータベースから読み出す。そして、ステップＳ１１２８において、ｐＢａｓｅ２３は、読み出したＰＭＤをサービスシステム２４に対して送信し、ステップＳ１１０６において、これが受信される。

【０２０３】

ステップＳ１１０７において、サービスシステム２４は、ステップＳ１１０６で取得されたＰＭＤに基づいて、各種の処理（サービス対応処理）を実行する。ステップＳ１１０７の処理の結果、ＰＭＤの変更が必要となる場合、サービスシステム２４は、ステップＳ１１０８において、ＰＭＤの内容を変更し、ｐＢａｓｅ２３に対して送信し、ステップＳ１１２９において、これが受信される。そして、ステップS１１３０において、ｐＢａｓｅ２３は、ステップＳ１１２９において受信されたＰＭＤが、サービスシステム２４に対応するサービスIDに対して変更許可のあるＰＭＤであるか否かを確認し、変更許可のあるＰＭＤである場合、記憶部１２８のデータベースの中の対応するＰＭＤの変更を行う（変更内容に更新する）。

【０２０４】

このようにして、ＰＭＤの読み出し、または変更を行う前に、ＰＫ２２に代わって、ｐＢａｓｅ２３が、図６の場合と同様に、サービスシステム２４との間でなりすましの確認を行うので、安全なサービスを提供することができる。

【０２０５】

次に図１９を参照して、図１７Ｃの場合の、ｐＢａｓｅ２３とサービスシステム２４との間の処理の流れの別の例を説明する。この例では、ＰＫ２２（のユーザ）に対応するＰ

ＭＤが、ｐＢａｓｅ２３の記憶部１２８に記憶されているものとし、サービスシステム２４との間で、なりすまし防止方法として、図７の場合と同様に公開鍵により暗号化された情報による認証が採用されているものとする。

【０２０６】

同図においては、ｐＢａｓｅ２３において、サービスシステム２４がなりすましではないことを確認し、その後サービスシステム２４において、ｐＢａｓｅ２３がなりすましではないことを確認する。そして、ｐＢａｓｅ２３とサービスシステム２４において、それぞれがなりすましではないことが確認できた後、ＰＭＤの読み出し、または変更の処理を行う。また、この例においては、ｐＢａｓｅ２３とサービスシステム２４は、RSAなどの公開鍵方式の暗号アルゴリズムによる情報の暗号化または複合化の処理を実行する機能を有しているものとする。なお、ＰＫ２２の秘密鍵、サービスシステム２４の公開鍵、ＰＫ２２のユーザＩＤ、およびサービスシステム２４のサービスＩＤは、ＰＫ２２のＰＭＤとしてｐＢａｓｅ２３の記憶部１２８の中のデータベースに記憶されているものとする。

【０２０７】

ステップＳ１８６１において、サービスシステム２４は、接続要求とサービスＩＤをｐＢａｓｅ２３に送信し、ステップＳ１８８１において、これが受信される。ステップＳ１８８２において、ｐＢａｓｅ２３は、図１０を参照して上述した場合と同様に、サービスＩＤマッチング処理を実行し、サービスＩＤの認識を行い、サービスＩＤに対応するユーザＩＤ、サービスシステム２４の公開鍵、ＰＫ２２の秘密鍵を取得する。

【０２０８】

ステップＳ１８８３において、ｐＢａｓｅ２３は、サービスシステム２４を認証するため、所定のコードで構成されるチャンレンジコードを生成し、チャレンジコードをサービスＩＤに対応する公開鍵（サービスシステム２４の公開鍵）で暗号化し、暗号化されたチャレンジコードとユーザＩＤをサービスシステム２４に送信し、ステップＳ１８６２において、これが受信される。

【０２０９】

ステップＳ１８６３において、サービスシステム２４は、ステップＳ１８６２で受信された、暗号化されたチャレンジコードをサービスシステム２４の秘密鍵により復号し、復号されたチャレンジコードをレスポンスコードとし、レスポンスコードをユーザＩＤに対応する公開鍵で暗号化してｐＢａｓｅ２３に対して送信し、ステップＳ１８８４において、これが受信される。

【０２１０】

ステップＳ１８８５において、ｐＢａｓｅ２３は、ステップＳ１８８４で取得された、暗号化されたレスポンスコードをＰＫ２２の秘密鍵で複合化し、ステップＳ１８８３で生成したチャレンジコードと比較して、チャレンジコードとレスポンスコードが一致しているか否かを判定し、チャレンジコードとレスポンスコードが一致しないと判定された場合、サービスシステム２４が、なりすましである可能性があると判定し、通信の拒否を表す拒否信号をサービスシステム２４に送信し、ステップＳ１８６４において、これが受信される。

【０２１１】

このように、通信を開始するとき、ｐＢａｓｅ２３からチャレンジコードが送信され、サービスシステム２４からチャレンジコードと一致するレスポンスコードが返信されなかった場合、ｐＢａｓｅ２３により、その通信は拒否される。

【０２１２】

一方、ステップＳ１８８５において、チャレンジコードとレスポンスコードが一致すると判定された場合、ｐＢａｓｅ２３は、ステップＳ１８８６において、サービスシステム２４がなりすましでないことが確認できたことを表すコード（ＯＫ）を、サービスシステム２４に送信し、ステップＳ１８６５において、これが受信される。

【０２１３】

ステップＳ１８６６において、サービスシステム２４は、ｐＢａｓｅ２３（ＰＫ２２）

を認証するため、所定のコードにより構成されるチャレンジコードを生成し、チャレンジコードをユーザＩＤに対応する公開鍵（ＰＫ２２の公開鍵）で暗号化し、暗号化されたチャレンジコードをｐＢａｓｅ２３に対して送信し、ステップＳ１８８７において、これが受信される。

【０２１４】

ステップＳ１８８８において、ｐＢａｓｅ２３は、ステップＳ１８８７で受信された、暗号化されたチャレンジコードをＰＫの秘密鍵で復号し、復号されたチャレンジコードをレスポンスコードとし、レスポンスコードをサービスＩＤに対応する公開鍵で暗号化し、サービスシステム２４に対して送信し、ステップＳ１８６７において、サービスシステム２４によりこれが受信される。

【０２１５】

ステップＳ１８６８において、サービスシステム２４は、ステップＳ１８６７で受信された、暗号化されたレスポンスコードを、サービスシステム２４の秘密鍵で復号し、復号されたレスポンスコードが、ステップＳ１８６６で生成されたチャレンジコードと一致するか否かを判定し、チャレンジコードとレスポンスコードが一致しないと判定された場合、ｐＢａｓｅ２３が、なりすましである可能性があると判定し、ｐＢａｓｅ２３に対して、通信の拒否を表す拒否信号を送信し、ステップＳ１８８９で、これが受信される。

【０２１６】

このように、通信を開始するとき、サービスシステム２４からチャレンジコードが送信され、ｐＢａｓｅ２３からチャレンジコードと一致するレスポンスコードが返信されなかった場合、サービスシステム２４により、その通信は拒否される。

【０２１７】

一方、ステップＳ１８６８において、チャレンジコードとレスポンスコードが一致すると判定された場合、サービスシステム２４は、ｐＢａｓｅ２３がなりすましでないことが確認できたと判定し、ステップＳ１８６９において、ｐＢａｓｅ２３に対してＰＭＤの読み出し要求を送信し、ステップＳ１８９０において、これが受信される。ステップＳ１８９１において、ｐＢａｓｅ２３は、サービスシステム２４から読み出し要求のあったＰＭＤが、サービスシステム２４に対応するサービスＩＤに対して、読み出しが許可されているＰＭＤであるか否かを確認し、読み出しが許可されているＰＭＤである場合、そのＰＭＤを記憶部１２８のデータベースから読み出す。そして、ステップＳ１８９２において、ｐＢａｓｅ２３は、読み出したＰＭＤをサービスシステム２４に対して送信し、ステップＳ１８７０において、サービスシステム２４により、これが受信される。

【０２１８】

ステップＳ１８７１において、サービスシステム２４は、ステップＳ１８７０で取得されたＰＭＤに基づいて、各種の処理（サービス対応処理）を実行する。ステップＳ１８７１の処理の結果、ＰＭＤの変更が必要となる場合、サービスシステム２４は、ステップＳ１８７２において、ＰＭＤの内容を変更し、ｐＢａｓｅ２３に対して送信し、ステップＳ１８９３において、これが受信される。そして、ステップＳ１８９４において、ｐＢａｓｅ２３は、ステップＳ１８９３において受信されたＰＭＤが、サービスシステム２４に対応するサービスＩＤに対して変更許可のあるＰＭＤであるか否かを確認し、変更許可のあるＰＭＤである場合、記憶部１２８のデータベースの中の対応するＰＭＤの変更を行う（変更内容に更新する）。

【０２１９】

このようにして、ＰＭＤの読み出し、または変更を行う前に、ＰＫ２２に代わって、ｐＢａｓｅ２３が、図７の場合と同様に、サービスシステム２４との間でなりすましの確認を行うので、安全なサービスを提供することができる。なお、図１９においては、公開鍵方式の暗号アルゴリズムにより、チャレンジコードとレスポンスコードを暗号化する例について説明したが、共通鍵方式の暗号アルゴリズムで、チャレンジコードとレスポンスコードが、暗号化されるようにしてもよい。

【０２２０】

図２０Ａ乃至Ｃは、ＰＭＤの詳細な構成例を示す図である。同図に示されるＰＭＤは、上述したように、あるサービスＩＤ（例えば、サービスＩＤ１）に関連付けられたメタデータの集合であり、そのメタデータの識別情報であるプロパティと、そのプロパティの内容が記述されている。プロパティ「ｎａｍｅ」は、サービスＩＤ１に対応するサービスシステム２４に対して提供されたユーザＩＤを示すものであり、その内容は「ｆｏｏ」と記述されている。

【０２２１】

図２０Ａにおいて、プロパティ「なりすまし防止方法」は、サービスＩＤ１に対応するサービスシステム２４との間で行われるなりすまし防止の処理の方法を示すものであり、その内容は、「公開鍵方式」と記述されおり、図５のステップＳ８２で生成される確認コードに対応する。プロパティ「サービス公開鍵」は、サービスＩＤ１に対応するサービスシステム２４の公開鍵を示すものであり、その内容として鍵のデータが記述されている。プロパティ「ＰＫ秘密鍵」は、ＰＫ２２の秘密鍵を示すものであり、その内容として鍵のデータが記述されている。

【０２２２】

なお、図２０Ｂに示されるように、プロパティ「なりすまし防止方法」の内容が「共通鍵方式」と記述されている場合、プロパティ「サービス公開鍵」とプロパティ「ＰＫ秘密鍵」に代わってプロパティ「共通鍵」がＰＭＤの中に生成され、その内容として鍵データが記述される。さらに、図２０Ｃに示されるように、プロパティ「なりすまし防止方法」の内容が「合言葉方式」と記述されている場合、プロパティ「サービス公開鍵」とプロパティ「ＰＫ秘密鍵」に代わってプロパティ「サービス合言葉」とプロパティ「ＰＫ合言葉」がＰＭＤの中に生成され、その内容としてそれぞれ、サービス合言葉とＰＫ合言葉が記述される。

【０２２３】

プロパティ「action」は、サービスＩＤ１に対応するサービスで実行される処理プログラムを示すものであり、その内容としてプログラムが記述されている。プロパティ「番組嗜好情報」は、サービスＩＤ１に対応するサービスで利用されるユーザの嗜好情報を示すものであり、その内容として、「スポーツ１０、バラエティ７、音楽５、その他３」が記述されている。

【０２２４】

アクセス制御は、そのプロパティの内容に対するアクセス制御情報を記述したものであり、各プロパティに対して、制御情報が設定される。制御情報は、所定のビット数で構成されるコードであり、例えば、次のように設定される。

【０２２５】

第１番目のビットにより、サービスＩＤ１に対応するサービスにおける当該プロパティの内容の読み出し可否が設定される。第２番目のビットにより、サービスＩＤ１に対応するサービスにおける当該プロパティの内容の変更可否が設定される。第３番目のビットにより、サービスＩＤ１以外のサービスＩＤに対応するサービスにおける当該プロパティの内容の読み出し可否が設定され、第４番目のビットにより、サービスＩＤ１以外のサービスＩＤに対応するサービスにおける当該プロパティの内容の変更可否が設定される。

【０２２６】

このほか、プログラムの実行可否を設定するビット、自由にアクセスすることが可能である（アクセス制限を設けない）ように設定するビットなどが設けられるようにしてもよい。なお、アクセス制御に設定される制御情報は、アクセス許可情報（図４）としてまとめて記憶されるようにしてもよい。

【０２２７】

次に、図２１を参照して、ＰＭＤ更新処理について説明する。この処理は、例えば、サービスシステム２４により、コンテンツの視聴サービスが提供された場合、図６のステップＳ２０７または図７のステップＳ４１１のサービス対応処理の１つとして、この処理がサービスシステム２４により実行される。

【０２２８】
ステップＳ１９０１において、ＣＰＵ１２１は、視聴された番組（コンテンツ）のメタデータを取得する。ステップＳ１９０２において、ＣＰＵ１２１は、メタデータのジャンルを分析する。ステップＳ１９０３において、ＣＰＵ１２１は、ステップＳ１９０２で分析されたジャンルがスポーツであるか否かを判定し、ジャンルがスポーツであると判定された場合、ステップＳ１９０４に進み、ＰＭＤの中のプロパティ「番組嗜好情報」の内容におけるスポーツのポイントをアップさせる。例えば、図２０において、「スポーツ１０、バラエティ７、音楽５、その他３」とされていたものが、「スポーツ１１、バラエティ７、音楽５、その他３」とされる。
【０２２９】
ステップＳ１９０３において、ステップＳ１９０２で分析されたジャンルがスポーツではないと判定された場合、ＣＰＵ１２１は、ステップＳ１９０５において、ジャンルがバラエティであるか否かを判定し、ジャンルがバラエティであると判定された場合、ステップＳ１９０６に進み、ＰＭＤの中のプロパティ「番組嗜好情報」の内容におけるバラエティのポイントをアップさせる。例えば、図２０において、「スポーツ１０、バラエティ７、音楽５、その他３」とされていたものが、「スポーツ１０、バラエティ８、音楽５、その他３」とされる。
【０２３０】
ステップＳ１９０５において、ステップＳ１９０２で分析されたジャンルがバラエティではないと判定された場合、ＣＰＵ１２１は、ステップＳ１９０７において、ジャンルが音楽であるか否かを判定し、ジャンルが音楽であると判定された場合、ステップＳ１９０８に進み、ＰＭＤの中のプロパティ「番組嗜好情報」の内容における音楽のポイントをアップさせる。例えば、図２０において、「スポーツ１０、バラエティ７、音楽５、その他３」とされていたものが、「スポーツ１０、バラエティ７、音楽６、その他３」とされる。
【０２３１】
ステップＳ１９０７において、ステップＳ１９０２で分析されたジャンルが音楽ではないと判定された場合、ＣＰＵ１２１は、ステップＳ１９０９に進み、ＰＭＤの中のプロパティ「番組嗜好情報」の内容におけるその他のポイントをアップさせる。例えば、図２０において、「スポーツ１０、バラエティ７、音楽５、その他３」とされていたものが、「スポーツ１０、バラエティ７、音楽５、その他４」とされる。
【０２３２】
このようにして、サービスシステム２４においてＰＭＤが更新される。更新されたＰＭＤは、ＰＫ２２に送信され、ＰＫ２２のＰＭＤが更新される。
【０２３３】
以上においては、サービスシステム２４により、ＰＭＤ更新処理が実行され、その更新に対応してＰＫ２２のＰＭＤが更新される例について説明したが、ＰＫ２２においてＰＭＤ更新処理が実行されるようにしてもよい。あるいはまた、ｐＢａｓｅ２３において、ＰＭＤ更新処理が実行され、ＰＫ２２のＰＭＤがｐＢａｓｅ２３のＰＭＤと同期されるようにしてもよい。
【０２３４】
また、異なるサービスにおいて利用されるＰＭＤの内容を組み合わせて新たにＰＭＤを生成することも可能である。例えば、サービスＩＤ１に対応するサービスと、サービスＩＤ２に対応するサービスが、ともに音楽に関するコンテンツを提供するサービスであり、図２２にしめされるようにサービスＩＤ１に対応するＰＭＤ３０１とサービスＩＤ２に対応するＰＭＤ３０２の中に、プロパティ「Ｒ＆Ｂ」、プロパティ「ｊａｚｚ」、およびプロパティ「ＰＯＰ」が存在しているものとする。
【０２３５】
この場合、ＰＭＤ３０１とＰＭＤ３０２が組み合わせられ、新しいＰＭＤ３０３が生成される。このとき、ＰＭＤ３０１のプロパティ「Ｒ＆Ｂ」の内容（１５）と、ＰＭＤ３０

２のプロパティ「Ｒ＆Ｂ」の内容（１７）が足し合わされ、新しいＰＭＤ３０３のプロパティ「Ｒ＆Ｂ」の内容が、「３２（＝１７＋１５）」に設定される。同様に、新しいＰＭＤ３０３のプロパティ「ｊａｚｚ」の内容は、「１０（＝５＋５）」に設定され、新しいＰＭＤ３０３のプロパティ「ＰＯＰ」の内容が「１５＝（１５＋０）」に設定される。

【０２３６】

このようにして、生成された新しいＰＭＤ３０３は、例えば、複数の音楽提供サービスのサービスＩＤに対応するＰＭＤとして生成され、ＰＫ２２のユーザの音楽に関する嗜好情報として利用される。

【０２３７】

また、サービスシステム２４（または、ｐＢａｓｅ２３）が、複数のＰＫ２２のＰＭＤの内容を組み合わせて新たにＰＭＤを生成することも可能である。図２３に、この場合の例を示す。１つのサービスシステム２４（または、ｐＢａｓｅ２３）を利用するＰＫとして、ＰＫ２２－１とＰＫ２２－２が存在し、ＰＫ２２－１のＰＭＤ３２１と、ＰＫ２２－２のＰＭＤ３２２の中に、プロパティ「Ｒ＆Ｂ」、プロパティ「ｊａｚｚ」、およびプロパティ「ＰＯＰ」が存在している。このとき、サービスシステム２４（または、ｐＢａｓｅ２３）は、ＰＭＤ３２１とＰＭＤ３２２を組み合わせて、新しいＰＭＤ３２３を生成する。

【０２３８】

このとき、ＰＭＤ３２１のプロパティ「Ｒ＆Ｂ」の内容（１５）と、ＰＭＤ３２２のプロパティ「Ｒ＆Ｂ」の内容（１７）が足し合わされ、新しいＰＭＤ３２３のプロパティ「Ｒ＆Ｂ」の内容が、「３２（＝１７＋１５）」に設定される。同様に、新しいＰＭＤ３２３のプロパティ「ｊａｚｚ」の内容は、「１０（＝５＋５）」に設定され、新しいＰＭＤ３２３のプロパティ「ＰＯＰ」の内容が「１５＝（１５＋０）」に設定される。

【０２３９】

このようにして、生成された新しいＰＭＤ３０３は、例えば、複数のユーザの共通するＰＭＤとして生成され、まだ嗜好情報が蓄積されていないＰＫ２２のユーザに対して、そのユーザの嗜好情報として提供される。

【０２４０】

また、ＰＫ２２に代えて別の機器から、サービスシステム２４を利用することも可能である。このような場合、図２４に示されるように、ユーザ２０は、ＰＫ２２を、ユーザ２０が指定する端末３６２と通信させ、コンテンツアクセスパッケージ３６１を、端末２６に送信される。そして、端末３６２がサービスシステム２４と通信を行う。コンテンツアクセスパッケージ３６１は、サービスシステム２４との通信を行うために必要な情報をまとめたパッケージであり、例えば、コンテンツのURI等のコンテンツを特定するユニークなID、コンテンツに関連する簡易な映像または文字列などにより構成されるアイコン、並びにサービスシステム２４との間でおこなわれるなりすまし防止の処理に用いられるＰＫ認証情報（例えば、ＰＫ２２の秘密鍵、ユーザＩＤなど）、およびサービス認証情報（例えば、サービスシステム２４の公開鍵、サービスＩＤなど）により構成される。

【０２４１】

このようにすることで、ユーザは、端末３６２を、あたかもＰＫ２２であるかのように（仮想のＰＫとして）利用することができる。

【０２４２】

次に、図２５乃至図２７を参照して、ＰＭＤを利用して、情報機器に自分の嗜好情報を反映させる（以下、パーソナライズと称する）例について説明する。図２５において、ＰＫ２２のユーザ２０が、所定の音楽データに基づいて、音楽の再生を行う音楽再生機器３８１と、インターネット２１に接続され、Ｗｅｂの閲覧などを行うパーソナルコンピュータ３８２を利用する。

【０２４３】

ユーザ２０は、ＰＫ２２のＰＭＤを利用して、音楽再生装置に、自分の好みの音楽を再生させることができる。この場合、ＰＫ２２は、音楽再生装置３８１を１つのサービスシ

ステムとして、インターネット２１を介さずに無線通信などにより、音楽再生装置３８１と通信する。このとき、図６または図７に示されるような処理が、ＰＫ２２と音楽再生装置３８１の間で行われる。このとき、例えば、図７のステップＳ４０９において、音楽再生装置３８１から音楽の嗜好情報のＰＭＤの読み出し要求が、ＰＫ２２に対して送信され、ステップＳ５０４で、ＰＫ２２から音楽の嗜好情報のＰＭＤが音楽再生装置３８１に対して送信される。そして、ステップＳ４１０で、音楽再生装置３８１が、ＰＫ２２からＰＭＤを取得すると、ステップＳ４１１のサービス対応処理として、ユーザの好みの音楽を再生する処理を実行する。この場合の音楽再生装置３８１の音楽再生処理について、図２６を参照して説明する。

【０２４４】

ステップＳ１９２１において、音楽再生装置３８１は、ＰＫ２２からＰＭＤを取得する。ステップＳ１９２２において、音楽再生装置３８１は、ステップＳ１９２１で取得されたＰＭＤの中の嗜好情報を分析する。ステップＳ１９２３において、音楽再生装置３８１は、嗜好情報に対応する音楽を再生する。

【０２４５】

このように、嗜好情報が含まれるＰＭＤを、音楽再生装置３８１に送信することで、好みの音楽を再生することができる。ＰＭＤは、ＰＫ２２に記憶されており、いろいろな場所に持ち運ぶことができるので、その場にある音楽再生装置を自分の好みの音楽を再生する音楽再生装置にパーソナライズすることが可能となる。

【０２４６】

また、図２５において、ユーザ２０は、ｐＢａｓｅ２３のＰＭＤを利用して、パーソナルコンピュータ３８２に、自分の好みのＷｅｂページを表示させることができる。この場合、ＰＫ２２は、サービスシステム２４－１０と、インターネット２１を介して通信する。このとき、図６または図７に示されるような処理が、ＰＫ２２とサービスシステム２４－１０の間で行われる。そして、サービスシステム２４－１０は、ＰＫ２２のユーザＩＤに基づいて、ユーザ２０のＰＭＤが記憶されているｐＢａｓｅ２３を特定し、ｐＢａｓｅ２３からユーザ２０のＰＭＤを取得する。このとき、図１８または図１９に示されるような処理が、サービスシステム２４―１０とｐＢａｓｅ２３の間で行われ、例えば、図１９のステップＳ１８６９において、サービスシステム２４－１０からＷｅｂの嗜好情報のＰＭＤの読み出し要求が、ｐＢａｓｅ２３に対して送信され、ステップＳ１８９１で、ｐＢａｓｅ２３からＷｅｂの嗜好情報のＰＭＤがサービスシステム２４－１０に対して送信される。

【０２４７】

ステップＳ１８７０で、サービスシステム２４－１０が、ｐＢａｓｅ２３からＰＭＤを取得すると、ステップＳ１８７１のサービス対応処理として、パーソナルコンピュータ３８２に対して、ユーザの好みに合ったＷｅｂサービスを提供する処理を実行する。この場合のサービスシステム２４－１０のＷｅｂ情報提供処理ついて、図２７を参照して説明する。

【０２４８】

ステップＳ１９４１において、サービスシステム２４－１０は、ＰＫ２２のユーザＩＤを取得する。ステップＳ１９４２において、サービスシステム２４－１０は、ステップＳ１９４１で取得されたユーザＩＤに対応するＰＭＤをｐＢａｓｅ２３から取得する。ステップＳ１９４３において、サービスシステム２４－１０は、ステップＳ１９４２で取得されたＰＭＤの嗜好情報を分析する。ステップＳ１９４４において、サービスシステム２４－１０は、嗜好情報に対応するＷｅｂサービスを提供する。

【０２４９】

あるいはまた、サービスシステム２４－１０がユーザのパーソナルコンピュータ３８２に作成するテキストファイルであるクッキーが、ＰＭＤとしてＰＫ２２またはｐＢａｓｅ２３に保存され、Ｗｅｂの閲覧を行う都度、パーソナルコンピュータ３８２にクッキーが送信されるようにしてもよい。

【０２５０】
このようにして、Ｗｅｂサービスが提供される。例えば、容量が大きいためＰＫ２２に記憶することができないＰＭＤをｐＢａｓｅ２３に記憶しておき、ｐＢｓｅ２３のＰＭＤに基づいて、パーソナルコンピュータなどの情報機器をパーソナライズすることができる。その結果、ユーザの嗜好をより適確に反映したパーソナライズを行うことができる。
【０２５１】
次に、図２８を参照して、ＰＭＤを利用して、情報機器をパーソナライズする別の例について説明する。同図において、家４００には、ユーザ２０－１乃至２０－３の３人のユーザが住んでおり、それぞれＰＫ２２－１乃至２２－３を所有している。家４００には、リビング４００－１、キッチン４００－２、および子供部屋４００－３の３つの部屋があり、それぞれの部屋には、各種の映像または音楽などのデータ（コンテンツ）を取得し、コンテンツを記憶または再生するコンテンツボックス４２１－１乃至４２１－３が設置されている。
【０２５２】
コンテンツボックス４２１－１乃至４２１－３は、ＬＡＮ４０２を介してルータ４０３と接続されており、ルータ４０３を介してインターネット２１に接続された各種のサーバと通信を行い、各種のコンテンツを取得する。
【０２５３】
また、コンテンツボックス４２１－１乃至４２１－３は、歩紋を検知するセンサが設けられており、ユーザがその近傍を通過すると歩紋検知してユーザを特定する。ルータ４０３は、インターネット２１からの不正なアクセスを防御するファイヤーウォール機能と、所定の容量のデータを記憶する記憶部を有している。ＬＡＮ４０２には、ＰＫを載置して充電を行うクレドール４０１が接続されており、クレドール４０１は、載置されたＰＫの情報をルータ４０３に送信する。
【０２５４】
ユーザ２０－１乃至２０－３は、外出時はＰＫ２２－１乃至２２－３を携帯し、家４００に帰宅するとクレドール４０１に自分が所有するＰＫを載置する。クレドール４０１は、ＰＫ２２－１乃至２２－３が載置されると、ＰＫ２２－１乃至２２－３のＰＭＤをルータ４０３に送信し、ルータ４０３は、インターネット２１を介してＰｂｓｅ２３と通信し、Ｐｂｓｅ２３からユーザ２０－１乃至２０－３のＰＭＤを取得し、記憶部に記憶する。なお、ユーザ２０－１乃至２０－３のＰＭＤには、ユーザ２０－１乃至２０－３の嗜好情報および歩紋情報が記憶されているものとする。
【０２５５】
コンテンツボックス４２１－１乃至４２１－３は、ルータ４０３からユーザ２０－１乃至２０－３の歩紋情報を取得し、近傍のユーザの好みにあったコンテンツの再生をおこなう。例えば、ユーザ２０－２がキッチンにいるとき、ユーザ２０－２の歩紋２０２－２を検知したコンテンツボックス４２１－２は、ルータ４０３からユーザ２０－２のＰＭＤを取得し、嗜好情報を分析し、自身が蓄積したコンテンツの中から嗜好情報に対応した音楽などを再生する。
【０２５６】
また、ユーザ２０－１と２０－３がリビング４００－１にいるとき、コンテンツボックス４２１－１は、ユーザ２０－１と２０－３の歩紋２０２－１と２０２－３を検知して、ルータ４０３から、ユーザ２０－１のＰＭＤと、ユーザ２０－３のＰＭＤを取得し、それぞれの嗜好情報を分析し、自身が蓄積したコンテンツの中から、例えば、ユーザ２０－１の好みにあった音楽を再生し、ユーザ２０－３の好みにあった映像を再生する。このように、家４００の中のコンテンツボックス４２１－１乃至４２１－３を、近傍のユーザに対応してパーソナライズすることができる。
【０２５７】
この例では、コンテンツボックス４２１－１乃至４２１－３をパーソナライズする例について説明したが、同様の方法で、各種のＣＥ機器などをパーソナライズすることも可能

であり、ユーザはＰＫを用いて所望の機器をパーソナライズすることができる。

【０２５８】

ところで、上述したようにルータ４０３は、ファイヤーウォール機能を有しているので、例えば、ＬＡＮ４０２に接続される機器とインターネット２１に接続される機器との通信が制約されている（例えば、コンテンツボックスとｐＢａｓｅの通信に利用できるプロトコル（ポート番号）が限られる）。このため、ＬＡＮ４０２に接続される機器とインターネット２１との通信は、図２９に示されるようにして行われる。最初に、コンテンツボックス４２１－１からｐＢａｓｅ２３に対して、矢印４４１に示されるようにhttps(SSL)プロトコルを使って、セッションを開始する。セッションが確立された後、コンテンツボックス４２１－１とｐＢａｓｅ２３は、点線４４２に示されるようにhttpsプロトコルでの通信を行う。

【０２５９】

また、図１７Ａを参照して上述したように、ＰＫ２２－１乃至２２－３とｐＢａｓｅ２３の間では、ＰＭＤの同期が行われる。図２８の例の場合、ＰＭＤの同期は、クレドール４０２およびコンテンツボックス４２１－１乃至４２１－３を介して行われる。ＰＫ２２－１、クレドール４０１、ｐＢａｓｅ２３、およびコンテンツボックス４２１－１の間でＰＭＤの同期が行われる場合の処理の流れについて、図３０を参照して説明する。

【０２６０】

ステップＳ２００１において、ＰＫ２２－１は、クレドール４０１に載置されると、自身のＰＭＤの内容をクレドール４０１に送信し、ステップＳ２０２１においてこれが受信される。ステップＳ２０２２において、クレドール４０１は、ステップＳ２０２１で受信された情報をｐＢａｓｅ２３に送信し、ステップＳ２０４１でこれが受信される。ステップＳ２０４２において、ｐＢａｓｅ２３は、図３１を参照して後述するＰＭＤ同期処理を実行する。これにより、ｐＢａｓｅ２３に記憶されているＰＭＤが更新され、ＰＫ２２－１のＰＭＤを更新する同期データが生成される。

【０２６１】

ステップＳ２０４３において、ｐＢａｓｅ２３は、同期データをクレドール４０１に送信し、ステップＳ２０２３で、これが受信される。ステップＳ２０２４において、クレドール４０１は、ステップＳ２０２３で受信された情報をＰＫ２２－１に送信し、ステップＳ２００２で、これが受信される。そして、ステップＳ２００３において、ＰＫ２２－１は、ステップＳ２００２で受信した同期データに基づいて、ＰＫ２２－１のＰＭＤを更新し、ＰＫ２２－１のＰＭＤとｐＢａｓｅ２３のＰＭＤの同期が行われる。

【０２６２】

コンテンツボックス４２１－１において、コンテンツが再生されると、ステップＳ２０６１において、コンテンツボックス４２１－１は、コンテンツの視聴履歴などの履歴情報をｐＢａｓｅ２３に送信し、ステップＳ２０４４で、これが受信され、ｐＢａｓｅ２３は、履歴情報に基づいてＰＭＤの嗜好情報を更新する。ステップＳ２０４５において、ｐＢａｓｅ２３は、ＰＭＤの更新結果を同期データとして、クレドール４０１に送信し、ステップＳ２０２５でこれが受信される。ステップＳ２０２６において、クレドール４０１は、ステップＳ２０２５で受信された情報をＰＫ２２－１に送信し、ステップＳ２００３で、これが受信され、ステップＳ２００５において、ＰＫ２２－１のＰＭＤが更新される。

【０２６３】

このようにしてＰＭＤの同期が行われる。

【０２６４】

次に、図３１を参照して、図３０のステップＳ２０４２のＰＭＤ同期処理の詳細について説明する。

【０２６５】

ステップＳ２０８１において、ＣＰＵ１２１は、図３０のステップＳ２０４１で受信したＰＭＤと、ｐＢａｓｅ２３に記憶されているＰＭＤの内容を比較する。このとき、ｐＢａｓｅ２３に記憶されているＰＭＤの中から、受信したＰＭＤに対応するＰＭＤが１つず

つ抽出されて比較され、そのＰＭＤが最後に更新された日時を表す更新日時の情報が比較される。

【０２６６】

ステップＳ２０８２において、ＣＰＵ１２１は、ステップＳ２０４１で受信したＰＭＤの更新日時が、ｐＢａｓｅ２３に記憶されているＰＭＤの更新日時より新しいか否かを判定し、受信したＰＭＤの更新日時が、ｐＢａｓｅ２３に記憶されているＰＭＤの更新日時より新しいと判定された場合、ステップＳ２０８３に進み、ｐＢａｓｅ２３に記憶されているＰＭＤの内容を受信したＰＭＤの内容に更新する。

【０２６７】

一方、ステップＳ２０８２において、ＣＰＵ１２１は、ステップＳ２０４１で受信したＰＭＤの更新日時が、ｐＢａｓｅ２３に記憶されているＰＭＤの更新日時より新しくないと判定された場合、ステップＳ２０８４に進み、ｐＢａｓｅ２３に記憶されているＰＭＤの内容を同期データとする。この同期データは、ＰＭＤ同期処理の終了後、ステップＳ２０４３（図３０）で、ＰＫ２２－１に送信され、ＰＫ２２－１において、同期データに基づくＰＭＤの更新が行われる。

【０２６８】

ステップＳ２０８３またはＳ２０８４の処理の後、ＣＰＵ１２１は、ステップＳ２０８５において、全てのＰＭＤをチェックしたか否かを判定し、まだ全てのＰＭＤをチェックしていないと判定された場合、ステップＳ２０８６に進み、次のＰＭＤをチェックする。その後処理は、ステップＳ２０８１に戻り、それ以降の処理が繰り返し実行される。

【０２６９】

ステップＳ２０８５において、全てのＰＭＤをチェックしたと判定された場合、処理は終了される。

【０２７０】

このようにして、ｐＢａｓｅ２３において、ＰＭＤの同期が行われる。

【０２７１】

次に、ＰＫに各種のカードの情報を保存して利用する例について図３２を参照して説明する。この例では、カード情報を有するＰＭＤ４６１がＰＫ２２に保存されているものとする。例えば、ユーザ２０が買い物をするとき、ＰＫ２２は、レジ４８１と無線通信などにより通信を行い、ＰＭＤ４６１の情報がレジ４８１に取得される。ＰＭＤ４６１は、ユーザ２０が保有するクレジットカードなどのカード１乃至カードＮのカード番号が記述されたカード情報を含むＰＭＤである。このとき、レジ４８１をサービスシステムとして、ＰＫ２２とレジ４８１の間で図６または図７に示されるような処理が行われる。そして、レジ４８１は、買い物代金の決済などを行うカード処理サーバ４８３とインターネット２１を介して通信し、代金を決済する。

【０２７２】

例えば、プリペイドカードの残高、カードの利用履歴などの情報は、インターネット２１を介して接続される、別のサーバのデータベース４８２－１乃至４８２－Ｎに記憶されており、カード処理サーバ４８３は、代金の決済を行った後、データベース４８２－１乃至４８２－Ｎの内容を更新する。

【０２７３】

このようにすることで、ＰＫ２２を仮想のカードケースとし、各種カードをカードケースにまとめて入れて、必要なときにそのカードを取り出して利用することができる。また、ＰＫ２２にカードリーダ機能を設けて、カードの情報を読み込ませ、その内容がＰＫ２２の近傍のレジ４８１に送信されるようにしてもよい。

【０２７４】

次に、図３３を参照して、ＰＫを利用して、ユーザの周辺の機器の制御を行う例について説明する。同図において、ユーザ２０は、ＰＫ２２を携帯すると同時に、タッチパッド付ディスプレイ５２１を有するコンソール端末５２１を携帯し、プロジェクター５０３が設置された会議室に入る。会議室には、アクセスポイント２５が設置されており、アクセ

スポイント２５は、インターネット２１に接続される。インターネット２１には、プロジェクター５０３など、アクセスポイント２５の周辺に存在する機器の制御情報を保有する環境サーバ５０１が接続されている。ユーザ２０は、ＰＫ２２を利用して、プロジェクター５０３の制御コードを取得し、コンソール端末５２１を操作して、プロジェクター５０３を制御する。

【０２７５】

このとき、環境サーバからプロジェクター５０３の制御コードを取得する処理の流れについて、図３４を参照して説明する。ステップＳ２１２１において、ＰＫ２２は、無線通信などによりコンソール端末５０２と通信を行い、コンソール端末５０２に対して機器情報の要求を送信し、ステップＳ２１０１においてこれが受信される。ステップＳ２１０２において、コンソール端末５０２は、自身の機器情報をＰＫ２２に送信し、ステップＳ２１２２でこれが取得される。

【０２７６】

また、ユーザが会議室に入るとＰＫ２２は、アクセスポイント２５と無線通信などにより通信を行い、アクセスポイント２５を経由して、環境サーバ５０１と通信を行う。このとき、環境サーバ５０１をサービスシステムとして図６または図７に示されるような処理が、ＰＫ２２と環境サーバ５０１の間で行われる。そして、ステップＳ２１２３において、ＰＫ２２は、コンソール端末５０２の機器情報を１つのＰＭＤとして、環境サーバ５０１に対して、制御コードの取得要求を送信し、ステップＳ２１４１でこれが受信される。ステップＳ２１４２において、環境サーバ５０１は、コンソール端末５０２にインストールするプロジェクター５０３の制御コードを、ＰＭＤに追加してＰＫ２２に送信し、ステップＳ２１２４でこれが受信される。

【０２７７】

その後、コンソール端末５０２をサービスシステムとして図６または図７に示されるような処理が、ＰＫ２２とコンソール端末５０２の間で行われる。そして、ステップＳ２１２５において、ＰＫ２２は、ステップＳ２１２４で受信したＰＭＤをコンソール端末５０２に対して送信し、ステップＳ２１０３でこれが受信され、プロジェクター５０３の制御コードがコンソール端末５０２にインストールされる。ユーザ２０は、タッチパッド付ディスプレイ５２１を操作して、プロジェクター５０３の制御を行う。

【０２７８】

このようにして、ＰＫを利用して、ユーザの周辺の機器の制御が行われる。このように、周辺の機器に対応して、適切な制御コードやデータなどを選択して送信することで、各種の機器を適正に制御することができる。

【０２７９】

また、ＰＫを利用した、ユーザの周辺の機器の制御の別の例として、図３５に示されるようなドアの開閉をおこなうこともできる。この例では、アクセスポイント２５の周辺にドア５４３と、ドア５４３のロックなどを解除してドア５４３の開放処理を行うドア開放制御機５４２が存在する。ドア開放制御機５４２は、インターネット２１を介して、ドア開放制御機５４２の制御コードを記憶しているサーバ５４１と接続されている。

【０２８０】

ユーザ２０が、サービスポイント２５と通信可能な範囲４１の中に入ると、サーバ５４１をサービスシステムとして、図６または図７に示されるような処理が行われ、ユーザ２０が携帯するＰＫ２２が、アクセスポイント２５を介して、インターネット２１に接続されているサーバ５４１と通信し、サーバ５４１は、ドア開放制御機５４２に対して、ドア５４３の開放処理を実行させるように制御する。

【０２８１】

この場合、例えば、ユーザ２０（ＰＫ２２）の近傍のドア５４３を特定するＩＤなどの情報が、ＰＭＤとして、サーバ５４１に送信され、サーバ５４１は、受信したＰＭＤに基づいて、ドア５４３を特定し、ドア開放制御機５４２に対して、ドア５４３の開放処理を実行させる制御する制御コードを送信する。

【０２８２】
このように、ユーザ２０がドア５４３の近くのアクセスポイント２５の近傍に行くと、自動的にドア５４３が開放されるようにすることができる。また、ＰＫ２２とサーバ５４１の間で、図６または図７に示されるようななりすまし防止の処理が行われるので、不正な侵入者などに対してドア５４３が開放されないようにすることができる。
【０２８３】
また、例えば、ドア５４３付近に守衛室などがあり、ドア５４３から不正な侵入者が入らないように守衛が監視している場合、例えば、図３６に示されるように、ＰＫ２２から、守衛室のパーソナルコンピュータ５６２に対して、ＩＤ番号と顔写真のデータが含まれるＰＭＤを送信し、パーソナルコンピュータ５６２に、ＰＭＤに対応する顔写真が表示されるようにすることで、さらにセキュリティを強化することができる。このようにすることで、ＰＫ２２（ユーザ２０）のＰＭＤに対応した顔写真が、パーソナルコンピュータ５６２に表示されるので、例えば、不正な侵入者が、盗んだＰＫ２２を使ってドア５４３から侵入しようとしても、顔写真と違う人物である（ユーザ２０ではない）ことが守衛に分かってしまうため、ドア５４３から侵入することができない。
【０２８４】
次に、図３７を参照して、ＰＫを利用して、周辺の機器を使った会話を行う例について説明する。この例においては、ユーザ２０－２が、ＰＫ２２－１を所有するユーザ２０－１との会話を希望しているものとする。そして、ＰＫ２２－１は、ｐＢａｓｅ２３と所定の時間間隔で通信を行い、図３１を参照して上述したようにＰＭＤの同期処理が行われているものとする。
【０２８５】
ユーザ２０－１の周囲には、アクセスポイント２５、電話機５８１、ならびにテレビ会議を行うとき利用するカメラ５８２とディスプレイ５８３が存在し、電話機５８１乃至ディスプレイ５８３の制御コードを記憶する環境サーバ５８４が、インターネット２１に接続されている。さらに、インターネット２１には、ｐＢａｓｅ２３と、会話の接続サービスを提供する会話接続サーバ６０１が接続されている。会話接続サーバ６０１は、ユーザ（例えば、ユーザ２０－２）から、特定の相手（例えば、ユーザ２０－１）に対する会話接続要求を受け付けて、相手の周辺の機器を使った会話を提供する。
【０２８６】
この場合、会話接続を行う処理の流れについて、図３８を参照して説明する。ＰＫ２２－１は、カメラ５８２乃至ディスプレイ５８３などの周辺機器をサービスシステムとし、図６または図７に示されるような処理を行い、周辺機器と通信する。そして、ステップＳ２２２１において、ＰＫ２２－１は、周辺機器に対して機器情報の要求を送信し、ステップＳ２２０１で、これが受信される。ステップＳ２２０２において、カメラ５８２乃至ディスプレイ５８３など周辺機器は、自身のＩＤまたはアドレスなどの機器情報をＰＫ２２－１にＰＭＤとして送信し、ステップＳ２２２２で、これが受信される。受信されたＰＭＤは、ステップＳ２２２３において、ユーザ２０－１が利用可能な機器を表すＰＭＤとしてｐＢａｓｅ２３に送信され、ステップＳ２２４１でこれが受信される（ＰＫ２２－１とｐＢａｓｅ２３で、ＰＭＤの同期が行われる）。
【０２８７】
一方、ユーザ２０－２から、ユーザ２０－１に対する会話の接続要求を受け付けた会話接続サーバ６０１は、ステップＳ２２６１において、ユーザ２０－１に対応するＰＭＤを保持するｐＢａｓｅ２３に対して、会話要求を送信し、ステップＳ２２４２で、これが受信される。このとき、会話接続サーバ６０１をサービスシステムとし、ｐＢａｓｅ２３が、ＰＫ２２－１の代わりとなって（代行して）、会話接続サーバ６０１とｐＢａｓｅ２３の間で、図６または図７に示されるような処理を行い通信が行われる。そして、ｐＢａｓｅ２３は、ステップＳ２２４３において、ユーザ２０－１が利用可能な機器を表すＰＭＤを会話接続サーバ６０１に対して送信する。
【０２８８】

ステップＳ２２６３において、会話接続サーバ６０１は、環境サーバ５８４を介して、周辺機器を制御し、ユーザ２０－１と２０－２の間で、電話機５８１による会話、またはカメラ５８２とディスプレイ５８３によるテレビ会議が行われる。このように、ＰＫを利用して、周辺の機器を使った会話が行われる。このようにすることで、ユーザ２０－１が、別の場所に行っても、ユーザ２０－１が利用可能な機器を表すＰＭＤに基づいて、会話を行うことができる。また、ＰＫ２２－１とｐＢａｓｅ２３の間で、所定の時間間隔（例えば、３０分間毎）にＰＭＤの同期が行われるので、ユーザは、いつでも、どこでも周辺機器を利用して会話を行うことができる。

【０２８９】

次に、ＰＫを利用してユーザの現在地を特定する例について、図３９を参照して説明する。この例では、ユーザ２０は、ＰＫ２２を携帯しており、ＰＫ２２は、近傍のアクセスポイント２５－１と通信する。アクセスポイント２５－１乃至２５－ｎは、スペースサーバ６４１と接続されており、スペースサーバ６４１は、ＰＫ２２が通信しているアクセスポイントのＩＤなどの情報を記憶する。また、スペースサーバ６４１は、インターネット２１と接続されており、インターネット２１には、ｐＢａｓｅ２３と、ユーザの現在地を特定するロケーションサーバ６４２が接続されている。

【０２９０】

この場合、インターネットに接続された機器６４３を用いて、ユーザの現在地を特定する処理の流れについて、図４０を参照して説明する。

【０２９１】

ＰＫ２２は、スペースサーバ６４１をサービスシステムとし、図６または図７に示されるような処理を行い、スペースサーバ６４１と通信する。そして、ステップＳ２３２１において、ＰＫ２２は、スペースサーバ６４１に対して、今、ＰＫ２２が通信しているアクセスポイントのＩＤの取得を要求し、ステップＳ２３０１において、これが受信される。ステップＳ２３０２において、スペースサーバ６４１は、アクセスポイント２５－１のＩＤをＰＭＤとして、ＰＫ２２に送信し、ステップＳ２３２２で、これが受信される。受信されたＰＭＤは、ステップＳ２３２３において、ユーザ２０の近傍のアクセスポイントを表すＰＭＤとしてｐＢａｓｅ２３に送信され、ステップＳ２３４１でこれが受信される（ＰＫ２２－１とｐＢａｓｅ２３で、ＰＭＤの同期が行われる）。

【０２９２】

一方、機器６４３は、ステップＳ２３８１において、ユーザ２０の現在地の取得要求をロケーションサーバ６４２に対して送信し、ステップＳ２３６１で、これが受信される。ステップＳ２３６２において、ロケーションサーバ６４２は、ユーザ２０のＰＭＤを保持するｐＢａｓｅ２３に対して、ユーザ２０の現在地の取得要求を送信し、ステップＳ２３４２で、これが受信される。このとき、ロケーションサーバ６４２をサービスシステムとし、ｐＢａｓｅ２３が、ＰＫ２２の代わりとなって（代行して）、ロケーションサーバ６４２とｐＢａｓｅ２３の間で、図１８または図１９に示されるような処理が行われ、通信が行われる。そして、ステップＳ２３４３において、ｐＢａｓｅ２３は、ユーザ２０の近傍のアクセスポイントを表すＰＭＤをロケーションサーバ６４２に対して送信し、ステップＳ２３６３で、これが受信される。

【０２９３】

ロケーションサーバ６４２は、ステップＳ２３６３で受信されたＰＭＤに基づいて、ユーザ２０の近傍のアクセスポイント（今の場合、アクセスポイント２５－１）の情報を取得し、そのアクセスポイントの位置を特定する。そして、ロケーションサーバ６４２は、アクセスポイント２５－１の近傍を、ユーザ２０の現在地とし、その現在地の情報を、ステップＳ２３８２において、機器６４３に送信し、ステップＳ２３８２で、これが受信される。

【０２９４】

このように、ＰＫを利用して、ユーザ２０の現在地が特定される。このようにすることで、ユーザ２０が、別の場所（例えば、アクセスポイント２５－２の近傍）に行っても、

ユーザ２０の近傍のアクセスポイントを表すＰＭＤに基づいて、現在地を正確に特定することができる。

【０２９５】

また、ユーザ２０の近傍のアクセスポイントを表すＰＭＤが、ＰＫ２２に記憶されるようにしてもよい。例えば、図４１に示されるように、ユーザ２０が旅行などで移動するとき、ＰＫ２２を携帯し、ＰＫ２２は、ユーザの現在地（近傍のアクセスポイントの情報）と、行き先のアドレスを含むＰＭＤ６６０を生成する。ユーザ２０は移動中に、地図情報を提供する端末６６１と、ＰＫ２２を通信させ、ＰＭＤ６６０を端末６６１に送信させる。これにより、例えば、端末６６１に、現在地から目的地までの道を案内する地図が表示される。

【０２９６】

また、ＰＭＤ６６０を方向表示機６６２に送信させ、進むべき方向が表示されるようにしてもよい。このようにＰＭＤ６６０を利用することで、ユーザにとって利便性の高い、道案内をすることができる。

【０２９７】

あるいはまた、このようにして特定されたユーザの現在地に基づいて、ユーザへのメッセージが伝達されるようにすることも可能である。例えば、インターネットに接続されたメールサーバが、スペースサーバ６４１からユーザの現在地の情報を取得し、図３７に示されるような方法で、ユーザが利用可能な機器に関する情報を取得して電子メールを送信することもできる。このようにすることで、例えば、ユーザが本社にいるときは、本社のパーソナルコンピュータに電子メールが送信され、ユーザが、支社に出張しているときは、支社のパーソナルコンピュータに電子メールが送信される。その結果、ユーザは、どこにいても確実に自分宛のメッセージを受け取ることができる。

【０２９８】

以上においては、ユーザの近傍のアクセスポイントの情報からユーザの現在地を特定する例について説明したが、より詳細に現在地を特定することもできる。例えば、図４２に示されるように、アクセスポイント２５の近傍にＰＫ２２－１を携帯するユーザ２０－１と、ＰＫ２２－２を携帯するユーザ２０－２がいる場合、ＰＫ２２－１または２２－２は、スペースサーバ６４１と通信し、ユーザ２０－１または２０－２の顔特徴情報を含むＰＭＤをスペースサーバ６４１に送信する。なお、ＰＫ２２－１または２２－２は、範囲４１の中において、アクセスポイント２５と通信することができるものとする。

【０２９９】

カメラ６８１は、アクセスポイント２５に近接して設置され、範囲４２の中にあるオブジェクトを撮影し、画像データを出力する。スペースサーバ６４１は、カメラ６８１と接続されており、カメラ６８１から出力される画像データを、ユーザ２０－１または２０－２の顔特徴情報と比較する。そして、顔特徴情報が一致する画像が検出された場合、スペースサーバ６４１は、ユーザ２０－１または２０－２は、アクセスポイント２５の近傍にいるものと判定し、アクセスポイント２５のＩＤをＰＫ２２－１または２２－２に送信する。

【０３００】

このようにすることで、ユーザ２０－１または２０－２の現在地を、アクセスポイントの近傍（範囲４１の中）から、さらに詳細に、カメラ６８１の近傍（範囲４２の中）として特定することができる。

【０３０１】

あるいはまた、カメラ６８１から出力される画像データが、ＰＭＤとしてｐＢａｓｅ２３に記憶され、ユーザの現在地の周辺の情報として、必要に応じてサービスシステムに提供されるようにしてもよい。このようにすることで、ユーザの正確な現在地を隠蔽しつつ、ユーザの周辺の映像を提供することができる。

【０３０２】

ところで、複数のアクセスポイントが、比較的近傍に設置されている場合、ＰＫ２２は

、通信すべきアクセスポイントを選択（検出）する必要がある。

【０３０３】

図４３を参照して、ＰＫ２２によるアクセスポイントの検出の例であるアクセスポイント検出処理１について説明する。ステップＳ２５０１において、ＰＫ２２は、通信出力のパワーを最小にする。上述したように、ＰＫ２２は、ＲＦ（Radio Frequency）通信、準静電界通信、光通信などの無線通信によりアクセスポイントと通信を行う。ステップＳ２５０１においては、例えば、ＰＫ２２の電波出力を最小に設定する。

【０３０４】

ステップＳ２５０２において、ＰＫ２２は、アクセスポイントが検出されたか否かを判定し、アクセスポイントが検出されなかったと判定された場合、ステップＳ２５０６に進み、通信出力のパワーが最大か否かを判定し、まだ最大ではないと判定された場合、ステップＳ２５０７に進み、通信出力のパワーを１段階上げる。そして、処理は、ステップＳ２５０２に戻り、それ以降の処理が繰り返し実行される。

【０３０５】

図４４を参照して、さらに詳しく説明する。ＰＫ２２は、通信パワーが最小出力の場合、範囲７０１に電波を出力することができる。アクセスポイント２５－１乃至２５－ｎは、ＰＫ２２からの電波を検知すると、応答を発信し、ＰＫ２２において、これが受信されることにより、ＰＫ２２がアクセスポイントを検出する。範囲７０１には、アクセスポイントがないため、ＰＫ２２は、アクセスポイントを検出できない。そこで、ＰＫ２２は、通信出力のパワーを１段階上げて、範囲７０２に電波を出力する。範囲７０２の中には、アクセスポイント２５－１が存在し、ＰＫ２２は、アクセスポイント２５－１を検出する。

【０３０６】

図４３に戻って、ステップＳ２５０２において、アクセスポイントが検出されたと判定された場合、ＰＫ２２は、ステップＳ２５０３に進み、検出されたアクセスポイント２５－１と通信する。

【０３０７】

一方、ステップＳ２５０６において、通信出力のパワーが最大であると判定された場合、ＰＫ２２の近傍にアクセスポイントはないものと判定され、ステップ２５０８において、エラー処理が実行され、アクセスポイント検出処理は終了される。

【０３０８】

このように、ＰＫ２２は、その通信出力を序所に上げていき、最初に見つかったアクセスポイントと通信する。このようにすることで、例えば、図４４において、ＰＫ２２は、アクセスポイント２５－２と通信しないようにできるので、通信による消費電力を抑制することができる。

【０３０９】

図４３においては、ＰＫ２２が、通信出力を変化させ、アクセスポイントを検出する例について説明したが、ＰＫの通信出力が同じでも、複数のアクセスポイントが検出される場合もある。そのような場合、アクセスポイントから発せられる通信出力（例えば、電界強度）に基づいて、アクセスポイントが検出されるようにしてもよい。図４５を参照して、ＰＫ２２によるアクセスポイントの検出の別の例であるアクセスポイント検出処理２について説明する。

【０３１０】

ステップＳ２５２１において、ＰＫ２２は、検出されたアクセスポイントの電界強度を取得する。ステップＳ２５２２において、ＰＫ２２は、電界強度が最も大きいアクセスポイントを検索する。ステップＳ２５２３において、ＰＫ２２は検索されたアクセスポイントと通信する。

【０３１１】

図４６を参照して、さらに詳しく説明する。範囲７１１－１において、アクセスポイント２５－１から出力される電波は電界強度１で、ＰＫ２２に受信される。範囲７１２－１

において、アクセスポイント２５－１から出力される電波は電界強度２で、ＰＫ２２に受信される。同様に、範囲７１１－２において、アクセスポイント２５－２から出力される電波は電界強度１で、ＰＫ２２に受信され、範囲７１２－２において、アクセスポイント２５－２から出力される電波は電界強度２で、ＰＫ２２に受信される。

【０３１２】

いま、ＰＫ２２は、アクセスポイント２５－１から出力される電波を電界強度１で受信しており、同時に、アクセスポイント２５－２から出力される電波を電界強度２で受信している。このような場合、複数のアクセスポイント（アクセスポイント２５－１と２５－２）の中から、電界強度が最も大きいアクセスポイントが検索される。いまの場合、アクセスポイント２５－１が検索され、ＰＫ２２は、アクセスポイント２５－１と通信する。

【０３１３】

このようにして、アクセスポイントが検出される。このようにすることで、例えば、ユーザがいる部屋とその部屋に隣接する部屋の両方にアクセスポイントが設置されている場合であっても、ＰＫ２２は、確実に、ユーザがいる部屋のアクセスポイントを利用した通信を行うことができる。

【０３１４】

なお、ＰＫの通信経路は１つに限られるものではなく、複数あってもよい。また、複数の通信経路において、それぞれ異なる方法で通信が行われるようにしてもよい。図４７は、ＰＫ２２の複数の通信経路を示す図である。

【０３１５】

同図において、ＰＫ２２は、範囲４１に電波を出力し、アクセスポイント２５とＲＦ通信を行う。そして、アクセスポイント２５を経由して、インターネット２１に接続され、サービスシステム２４－２と通信が行われる。一方、ＰＫ２２は、光通信用のインタフェース７６２を有する近傍のパーソナルコンピュータ７６１と光通信を行う。この場合、例えば、赤外線のような指向性のある光が、矢印７８１に沿ってＰＫ２２とパーソナルコンピュータ７６１から照射される。

【０３１６】

また、ユーザ２０が、準静電界通信用のインタフェース７６２の上にいるとき、ＰＫ２２は、矢印７８２に示されるように、インタフェース７６２と準静電界通信を行う。インタフェース７６２は、サービスシステム２４－１と接続されており、ＰＫ２２は、インタフェース７６２を経由して、サービスシステム２４－１と通信を行う。

【０３１７】

例えば、図３９に示されるように、ユーザの現在地を特定する場合、ユーザ（ＰＫ２２）の現在地が、ＲＦ通信のアクセスポイント２５の位置情報ではなく、準静電界通信用のインタフェース７６２の位置情報に基づいて、特定されるようにすれば、ユーザの現在地をより詳細に特定することができる。また、指向性の高い光通信用のインタフェース７６２の位置情報に基づいて、ユーザの現在地が特定されるようにすれば、さらに正確にユーザの現在地を特定することができる。例えば、会議室の机に、光通信用のインタフェース７６２を複数設けておき、着座したユーザが、それぞれが所持するＰＫを光通信用のインタフェース７６２と光通信させるようにすれば、どの席にどのユーザが着座したのかを正確に把握することができる。

【０３１８】

あるいはまた、図５に示されるようなサービスシステム２４の初期登録を行う場合の通信と、その後の通信で、異なる通信経路が設定されるようにしてもよい。例えば、サービスシステム２４の初期登録を行う場合、ＰＫ２２とサービスシステム２４の間で、まだなりすまし防止方法が定められていないので、ＰＫ２２が光通信などの通信が傍受され難い通信により、サービスシステム２４と直接通信して初期登録を行い、その後の通信は、ＲＦ通信により、インターネット２１を介してサービスシステム２４と通信するようにしてもよい。このようにすることで、より安全なサービスを提供することができる。

【０３１９】

上述したようにＰＫは小型のコンピュータであり、ＰＫ自身にプログラムを実行させ、所定の処理（例えば、受信した電子メールを表示させる処理）を行うようにすることも可能である。図４８と図４９を参照して、ＰＫにプログラムを実行させ、所定の処理を行う例について説明する。

【０３２０】

図４８において、ＰＫがＰＭＤ８０１を有しているものとする。ＰＭＤ８０１のプロパティ「プログラム」は、ＰＫ２２が実行するプログラムを表すものであり、その内容として、プログラムコードの実体が記憶されている。プロパティ「ｎａｍｅ」は、ＰＫのユーザＩＤを表すものであり、その内容は、「ｆｏｏ」とされている。プロパティ「ｐｕｓｈ」は、処理すべきデータ（例えば受信した電子メール）を表すものであり、その内容として、「緊急の連絡あり・・・」が記述されている。

【０３２１】

次に、図４９を参照して、ＰＫ２２がプログラムを実行する処理について説明する。この処理は、所定の周期（例えば、１時間毎）に行われるようにしてもよいし、ユーザの指令に基づいて、実行されるようにしてもよい。ユーザの指令は、例えば、ＰＫ２２の入力部１０６を構成するスイッチが、所定の回数押下されることにより行われる。ステップＳ２５４１において、ＣＰＵ１０１は、ＰＭＤ８０１のプロパティ「ｐｕｓｈ」にデータがあるか否かを判定し、データがあると判定された場合、ステップＳ２５４２に進み、プロパティ「ｐｕｓｈ」の内容をディスプレイに表示させる。いまの場合、「緊急の連絡あり・・・」が表示される。ステップＳ２５４３において、ＣＰＵ１０１は、プロパティ「ｐｕｓｈ」の内容を消去する。

【０３２２】

ステップＳ２５４１において、データがないと判定された場合、処理は終了される。

【０３２３】

このようにして、ＰＫ自身にプログラムを実行させ、例えば、受信した電子メールを表示させる処理が実行される。例えば、ＰＫを１つのサービスシステムとして、別のＰＫとの間で、図６または図７に示されるような処理が行われ、電子メールの送受信を行うようにすれば、なりすまし防止処理により、ユーザを正確に認証することができるので、電子メールのセキュリティをより向上させることができる。

【０３２４】

また、ｐＢａｓｅ２３を１つのサービスシステムとして、ＰＫ２２と通信させ、ｐＢａｓｅ２３からの要求に基づいて、ＰＫ２２がプログラムを実行することも可能である。この場合の処理の流れについて、図５０を参照して説明する。同図は、図７に対応しており、図７のサービスシステム２４に代わってｐＢａｓｅ２３とされている。

【０３２５】

図５０のステップＳ２８０１乃至Ｓ２８０８の処理は、図７のステップＳ４０１乃至Ｓ４０８の処理と同様の処理なので、その説明は省略する。図５０のステップＳ２８２１乃至Ｓ２８３６の処理は、図７のステップＳ４２１乃至Ｓ４３６と同様の処理なので、その説明は省略する。図５０のステップＳ２８８１乃至Ｓ２８９１は、図７のステップＳ４８１乃至Ｓ４９１と同様であり、図５０のステップＳ２９０１とＳ２９０２は、図７のステップＳ５０１とＳ５０２と同様なのでその説明は省略する。

【０３２６】

ステップＳ２８０９において、ｐＢａｓｅ２３は、ＰＫ２２に対して、プログラムの実行要求を送信し、ステップＳ２８３５において、ＰＫ２２の通信モジュール６１によりこれが受信される。ステップＳ２８３６において、通信モジュール６１は、ステップＳ２８３５で受信された内容を、ＤＢアクセスモジュール６６を経由してプログラムに対して出力し、ステップＳ２９２１において、これが受信されプログラムが実行される。

【０３２７】

このようにして、ｐＢａｓｅ２３からの要求に基づいて、ＰＫ２２のプログラムが実行される。

【０３２８】
なお、図５０においては、ｐＢａｓｅ２３を１つのサービスシステムとして、ＰＫ２２と通信させる例について説明したが、ＰＫ２２－１が、別のＰＫであるＰＫ２２－２を１つのサービスシステムとし、ＰＫ２２－２と通信を行うことも可能である。

【０３２９】
ところで、ＰＫ２２は、ユーザが携帯するものなので、バッテリーなどにより電力が供給される。このため、通信に用いられる電力は最小限にすることが望ましい。図５１を参照して、ＰＫ２２の通信スタンバイ処理について説明する。

【０３３０】
ステップＳ３１０１において、ＣＰＵ１０１は、待ちうけモードで通信する。このとき、ＰＫ２２においては、例えば、図４７に示した複数の通信経路のうち、最も消費電力が少ない準静電界通信のみが行われる。ステップＳ３１０２において、ＣＰＵ１０１は、通信があったか否かを判定し、通信があったと判定された場合、ステップＳ３１０３において、８０２．１１ｂによるＲＦ通信を起動する。ステップＳ３１０４において、ＣＰＵ１０１は、所定の時間が経過したか否かを判定し、所定の時間が経過したと判定されるまで待機する。

【０３３１】
ステップＳ３１０４において、所定の時間が経過したと判定された場合、ＣＰＵ１０１は、ステップＳ３１０５に進み、８０２．１１ｂによるＲＦ通信を終了する。その後、処理は、ステップＳ３１０１に戻り、それ以降の処理が繰り返し実行される。

【０３３２】
図５２と図５３を参照してさらに詳しく説明する。図５２において、ユーザ２０が、準静電界通信用のインタフェース８２１－１乃至８２１－３の上にいるとき、ＰＫ２２は、インタフェース７６２と準静電界通信を行う。サービスシステム８２２は、インタフェース８２１－１乃至８２１－３と接続されており、常に、サービスＩＤとサービス情報により構成されるパケット８２３をインタフェース８２１－１乃至８２１－３に送信している。いま、ユーザ２０が、インタフェース８２１－１の上にいるので、ＰＫ２２は、パケット８２３を受信し、通信があったと判定する（図５１のステップＳ３１０２）。

【０３３３】
そして、ＰＫ２２は、ＲＦ通信を起動し（図５１のステップＳ３１０３）、図５３に示されるように、範囲４１の中にあるアクセスポイント２５と通信を行い、アクセスポイント２５を経由して、サービスシステム８２２との通信を行う。

【０３３４】
このようにすることで、通常（待ち受けモード時）は、ＲＦ通信と比較して消費電力の少ない準静電界通信を行い、サービスシステム８２２と通信する必要があるときだけ、準静電界通信と比較して通信速度が高いＲＦ通信を用いて高速通信を行うようにすることができ、消費電力を抑制し、効率よく通信することができる。

【０３３５】
次に、ＰＫまたはｐＢａｓｅにより、実現されるサービスを複数組み合わせた例について、図５４乃至図５８を参照して説明する。図５４Ａにおいて、ＰＫ２２を携帯したユーザが、アクセスポイントが設置された部屋にはいると、ｐＢａｓｅ２３からユーザ２０に対する連絡内容が送信される。これにより、例えば、ＰＫ２２のディスプレイに「Ａさんから連絡あり」のメッセージが表示される。あるいはまた、図５４Ｂに示されるように、部屋８８１の中の床に設置された表示装置８８２が点灯することにより、ユーザ２０に対してメッセージがあることが通知されるようにしてもよい。

【０３３６】
自分に対する連絡があることを知ったユーザ２０は、ＰＫ２２をパーソナルコンピュータ９０１と通信させ、図５５に示されるように、パーソナルコンピュータ９０１に、ｐＢａｓｅ２３からコミュニケーションリストを含むＰＭＤを取得させ、コミュニケーションリストを表示させる。コミュニケーションリストは、ユーザ２０に対して、連絡があった

人の一覧を記述したリストであり、例えば、人物Ａ乃至Ｄの４人からの連絡があったことが記述されている。

【０３３７】

人物Ａ乃至ＤもそれぞれＰＫを所持しており、図３９に示されるような方法で、それぞれの現在地が特定され、コミュニケーションリストには、たとえば、人物Ａは移動中であり、人物Ｂは自席におり、人物Ｃは会議室Ｃにおり、人物Ｄは伝言を残している旨が表示される。

【０３３８】

例えば、会議室にいる人物Ｃと連絡をとりたいとき、ユーザ２０は、近傍の会議室Ａに入り、会議室Ｃとテレビ会議を行う。図５６に示されるように、会議室Ａには、電子ドキュメントなどを表示するモニタ９２１、相手の顔を表示するモニタ９２２、会議室Ｃの全体の様子を表示するモニタ９２３、およびタッチパッド付ディスプレイを備えたコンソール端末９２４が設置されている。

【０３３９】

このとき、ユーザ２０は、図３３に示されるような方法で、コンソール端末９２４にモニタ９２１乃至９２３の制御コードをインストールし、コンソール端末９２４を操作して、モニタ９２１乃至９２３を制御する。

【０３４０】

ここで、図５７に示されるように、会議室Ｃに、人物Ｃ、および人物Ｆ乃至Ｉの６人がいる場合、各人物が、それぞれ自分のＰＫを所有しているものとし、各自のＰＫを会議室Ｃの机に設置された光通信装置と通信させる。光通信は、指向性が強いので、ＰＫの存在する場所を正確に特定することができる。これにより、例えば、会議室Ａのコンソール端末９２４に人物Ｃ、および人物Ｆ乃至Ｉの名前、所属、および着席位置などが表示される。

【０３４１】

このように、ＰＫとｐＢａｓｅにより、ユーザにとって利便性の高いコミュニケーションの仕組を提供することができる。

【０３４２】

図５８は、ＰＫ２２とｐＢａｓｅ２３の組み合わせによるIP電話機９６１の待ちうけ電力を抑制する例を説明する図である。ＰＫ２２を携帯したユーザ２０の近傍に、アクセスポイント２５と、IP電話機９６１があり、IP電話機９６１は、インターネット２１に接続され、所定の相手と通話を行う。なお、消費電力抑制のために、IP電話機９６１は、通常電源がＯＦＦの状態にされている。

【０３４３】

この場合、ＰＫ２２は、アクセスポイント２５を介して、ｐＢａｓｅ２３と通信を行い、図３７に示されるような方法で、ユーザ２０が利用可能な機器を表すＰＭＤをｐＢａｓｅ２３に送信する（図５８の矢印１００１）。ユーザ２０との会話を希望する機器９８１は、インターネット２１の会話接続サーバに対して会話接続要求を行い、会話接続要求が、ｐＢａｓｅ２３に送信される（図５８の矢印１００２）。ｐＢａｓｅ２３は、ＰＫ２２と通信し、会話接続要求を通知する（図５８の矢印１００３）。この結果、図４９を参照して上述したように、ＰＫ２２のディスプレイに接続要求が表示される。

【０３４４】

ユーザ２０が、会話接続要求があることを知り、ＩＰ電話機９６１の電源をＯＮにすると、ＩＰ電話機９６１が利用可能となったことがｐＢａｓｅ２３に送信される（図５８の矢印１００４）。さらに、ｐＢａｓｅ２３から機器９８１に対してＩＰ電話機９６１が利用可能となったことが通知される（図５８の矢印１００５）これにより、機器９８１とＩＰ電話機９６１による通話が開始される。

【０３４５】

このようにして、ユーザ２０は、消費電力を抑制しながらＩＰ電話機９６１を利用することができる。

【０３４６】
以上においては、ＰＫ２２を、ユーザが携帯可能な小型のコンピュータとして説明したが、図４のソフトウェア６０を、例えば、汎用のパーソナルコンピュータなどに実装することにより、汎用のパーソナルコンピュータがＰＫとして利用されるようにすることも可能である。

【０３４７】
図５９は、ＰＫ２２のソフトウェア６０を、ユーザが持ち歩く携帯機器１１０１と１１０２に実装する例を示す図である。同図において、携帯機器１１０１と１１０２は、ユーザが所望する音楽データを再生する、例えばウォークマン（商標）のような小型の音楽再生装置である。携帯機器１１０１と１１０２には、ＰＫ２２のソフトウェア６０が実装されているとともに、ユーザの嗜好情報に適合する音楽データの取得または送信を行うサービスシステムであるサービスシステム２４－２０のソフトウェアが実装されている。

【０３４８】
すなわち、携帯機器１１０１と１１０２は、ＰＫ２２とサービスシステム２４－２０を1つの情報処理装置として実現したものであり、ユーザは、通信によるデータの授受を行うことなく、サービスの提供を受けることができる。この結果、ユーザは、どこに行っても、携帯機器１１０１または１１０２に蓄積されたＰＭＤの嗜好情報に基づいて、自分の好みに合う音楽を聴くことができる。

【０３４９】
また、携帯機器１１０１と１１０２に通信機能を設けるようにしてもよい。このようにすることで、例えば、携帯機器１１０１のユーザ２２－１１と、携帯機器１１０２のユーザ２２－１２が道で会ったとき、自分の好みに合う音楽の音楽データを交換し合うことができる。

【０３５０】
なお、図２５においては、ユーザのＰＭＤの中の嗜好情報に基づいて、パーソナライズが行われる例について説明したが、例えば、ネットワークに接続される他のサーバにおいて、ユーザの嗜好が既に分析されている場合、その分析結果と合わせて、より詳細なパーソナライズを行うことも可能である。図６０において、インターネット２１に接続されるサービスシステム２４－２１は、ＰＫ２２のユーザの嗜好情報に基づいて、テレビ番組を推薦する。一方、インターネット２１には、協調フィルタリングによりユーザの嗜好を分析する協調フィルタリングサーバ１２０１が接続されている。

【０３５１】
協調フィルタリングサーバ１２０１は、ｐＢａｓｅ２３からユーザのＰＭＤを取得し、ＰＭＤに含まれる視聴（操作）履歴を分析する。そして、あるユーザの視聴履歴に対して、他のユーザの視聴履歴との間でマッチングを取り、当該ユーザと視聴履歴の類似する他のユーザの視聴履歴を取得する。そして、視聴履歴が類似する（好みが似ている）他のユーザが視聴した番組で、当該ユーザが未だ視聴していない番組名を取得し、推薦する。

【０３５２】
このようにして協調フィルタリングサーバ１２０１により推薦される番組を、サービスシステム２４－２１が、ＰＫ２２のＰＭＤに基づいて、さらに選択し、ユーザに推薦する。このようにすることで、ユーザに対して、より嗜好に適合する番組を推薦することができる。

【０３５３】
勿論、協調フィルタリングサーバ１２０１により推薦される番組が直接ユーザに推薦されるようにしてもよい。上述したように、ＰＫ２２またはｐＢａｓｅ２３により、ユーザのＰＭＤの中に嗜好情報が既に蓄積されているので、ＰＫ２２またはｐＢａｓｅ２３を用いずに、ユーザが使用する機器（例えば、テレビジョン受像機など）の視聴履歴などから直接嗜好情報を収集して、番組の推薦を行う場合と比較して、協調フィルタリングサーバ１２０１の処理負荷を軽減することができる。

【０３５４】

なお、本明細書において上述した一連の処理を実行するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【図面の簡単な説明】

【０３５５】

【図１】本発明のサービス提供システムの構成例を示す図である。

【図２】図１のＰＫの構成例を示すブロック図である。

【図３】図１のｐＢａｓｅの構成例を示すブロック図である。

【図４】図１のＰＫのソフトウェアの構成例を示すブロック図である。

【図５】サービスＩＤの初期登録を行う処理の流れを示すアローチャートである。

【図６】ＰＫとサービスシステムにおいて、なりすまし防止を行う処理の流れを示すアローチャートである。

【図７】ＰＫとサービスシステムにおいて、なりすまし防止を行う処理の流れを示すアローチャートである。

【図８】鍵管理処理を説明するフローチャートである。

【図９】サービスＩＤ登録処理を説明するフローチャートである。

【図１０】サービスＩＤマッチング処理を説明するフローチャートである。

【図１１】ＰＫによりユーザの認証が行われる例を示す図である。

【図１２】ユーザ認証処理１を説明するフローチャートである。

【図１３】ユーザ認証処理２を説明するフローチャートである。

【図１４】ＰＭＤ管理処理を説明するフローチャートである。

【図１５】ＰＫの外部の機器を利用して、入出力インタフェースを構成する例を示す図である。

【図１６】ＰＫにより、周辺機器へのアクセスキーが隠蔽される様子を示す図である。

【図１７】ＰＫ、ｐＢａｓｅ、およびサービスシステム間の通信のパターンを示す図である。

【図１８】ｐＢａｓｅとサービスシステムにおいて、なりすまし防止を行う処理の流れを示すアローチャートである。

【図１９】ｐＢａｓｅとサービスシステムにおいて、なりすまし防止を行う処理の流れを示すアローチャートである。

【図２０Ａ】ＰＭＤの構成例を示す図である。

【図２０Ｂ】ＰＭＤの構成例を示す図である。

【図２０Ｃ】ＰＭＤの構成例を示す図である。

【図２１】ＰＭＤ更新処理を説明するフローチャートである。

【図２２】複数のＰＭＤに基づいて生成される新しいＰＭＤを示す図である。

【図２３】複数のＰＭＤに基づいて生成される新しいＰＭＤを示す図である。

【図２４】コンテンツアクセスパッケージの構成例を示す図である。

【図２５】ＰＫにより、各種の機器をパーソナライズする例を示す図である。

【図２６】音楽再生処理を説明するフローチャートである。

【図２７】Ｗｅｂ情報提供処理を説明するフローチャートである。

【図２８】ＰＫにより、各種の機器をパーソナライズする例を示す図である。

【図２９】ファイヤーウォール機能をもつルータを挟んで通信を行う例を示す図である。

【図３０】ＰＭＤの同期の処理の流れを示すアローチャートである。

【図３１】ＰＭＤ同期処理を説明するフローチャートである。

【図３２】ＰＫに各種カード情報を保持させて利用する例を示す図である。

【図３３】コンソール端末に制御コードをインストールする例を示す図である。

【図３４】制御コードを取得する処理の流れを示すアローチャートである。

【図３５】ＰＫによりドアを開放する例を示す図である。

【図３６】ＰＫの顔特徴情報が端末に表示される例を示す図である。
【図３７】会話接続サービスの例を示す図である。
【図３８】会話接続が行われる処理の流れを示すアローチャートである。
【図３９】ＰＫを利用して、ユーザの位置を特定する例をしめす図である。
【図４０】ユーザの位置を特定する処理の流れを示すアローチャートである。
【図４１】地図情報サービスを提供する例を示す図である。
【図４２】カメラを用いて、ユーザの位置を特定する例を示す図である。
【図４３】アクセスポイント検出処理１を説明するフローチャートである。
【図４４】アクセスポイントが検出される仕組を示す図である。
【図４５】アクセスポイント検出処理２を説明するフローチャートである。
【図４６】アクセスポイントが検出される仕組を示す図である。
【図４７】ＰＫの複数の通信ルートを示す図である。
【図４８】ＰＭＤの構成例を示す図である。
【図４９】ＰＫがプログラムを実行する処理を説明するフローチャートである。
【図５０】ｐＢａｓｅをサービスシステムとして、処理が行われる流れを示すアローチャートである。
【図５１】通信スタンバイ処理を説明するフローチャートである。
【図５２】待ち受け時の通信の例を示す図である。
【図５３】ＲＦ通信が行われる例を示す図である。
【図５４】ＰＫにより、ユーザにメッセージを通知する例を示す図である。
【図５５】コミュニケーションリストの例を示す図である。
【図５６】会議室内の機器を示す図である。
【図５７】会議室内の着席位置を示す図である。
【図５８】ＩＰ電話機の消費電力を抑制する例を示す図である。
【図５９】ＰＫのソフトウェアとサービスシステムのソフトウェアを１つの機器に実装する例を示す図である。
【図６０】協調フィルタリングサーバと、ＰＭＤを用いてパーソナライズを行う例を示す図である。

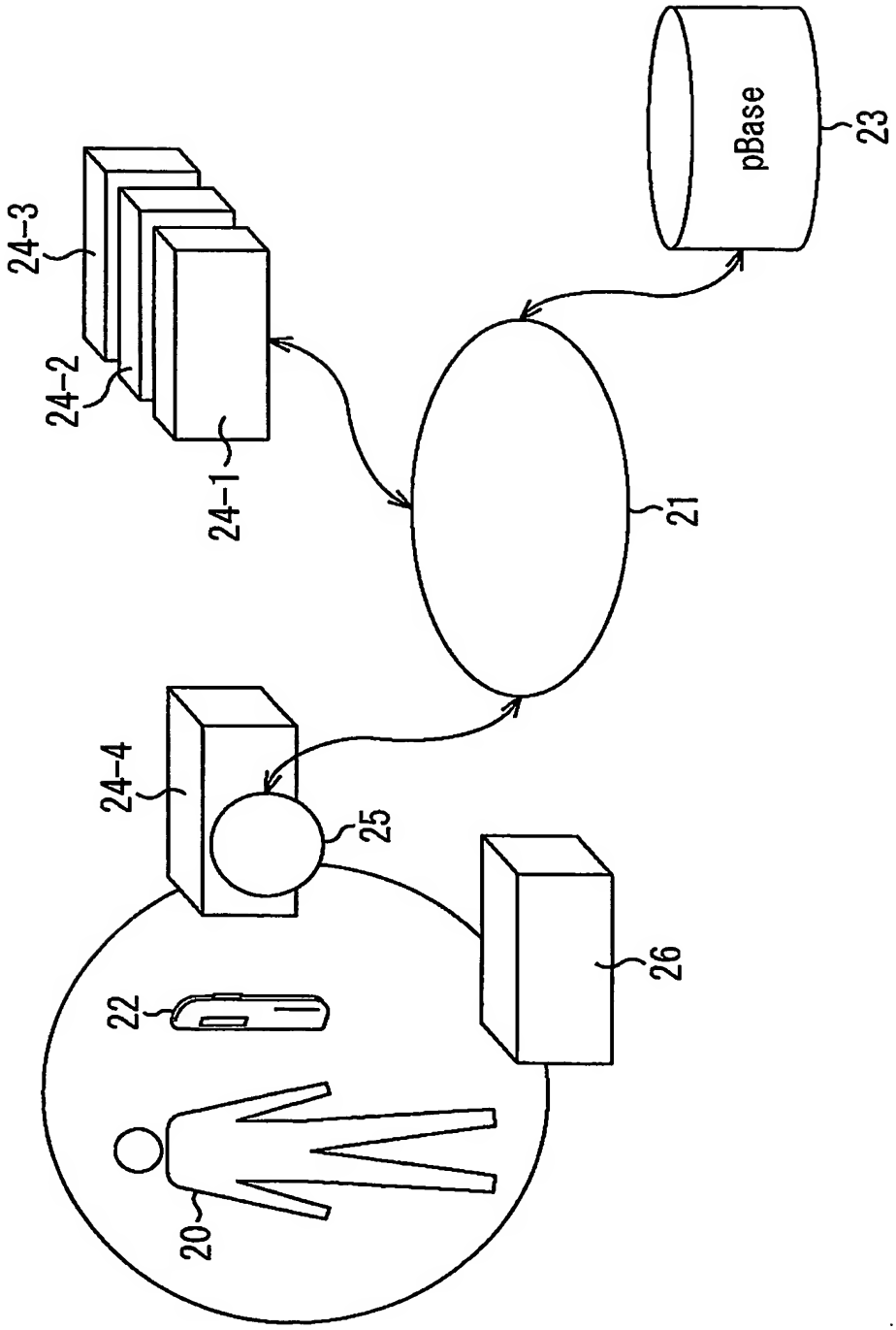
【符号の説明】

【０３５６】

２２　ＰＫ，　２３　ｐＢａｓｅ，　２４　サービスシステム，　６２　ユーザ制御許可入力モジュール，　６４　なりすまし防止モジュール，　６６　ＤＢアクセスモジュール，　６７ＰＭＤＢ，　１０１　ＣＰＵ，　１０６　入力部，　１０７　出力部，　１２１　ＣＰＵ，　１２６　入力部，　１２７　出力部

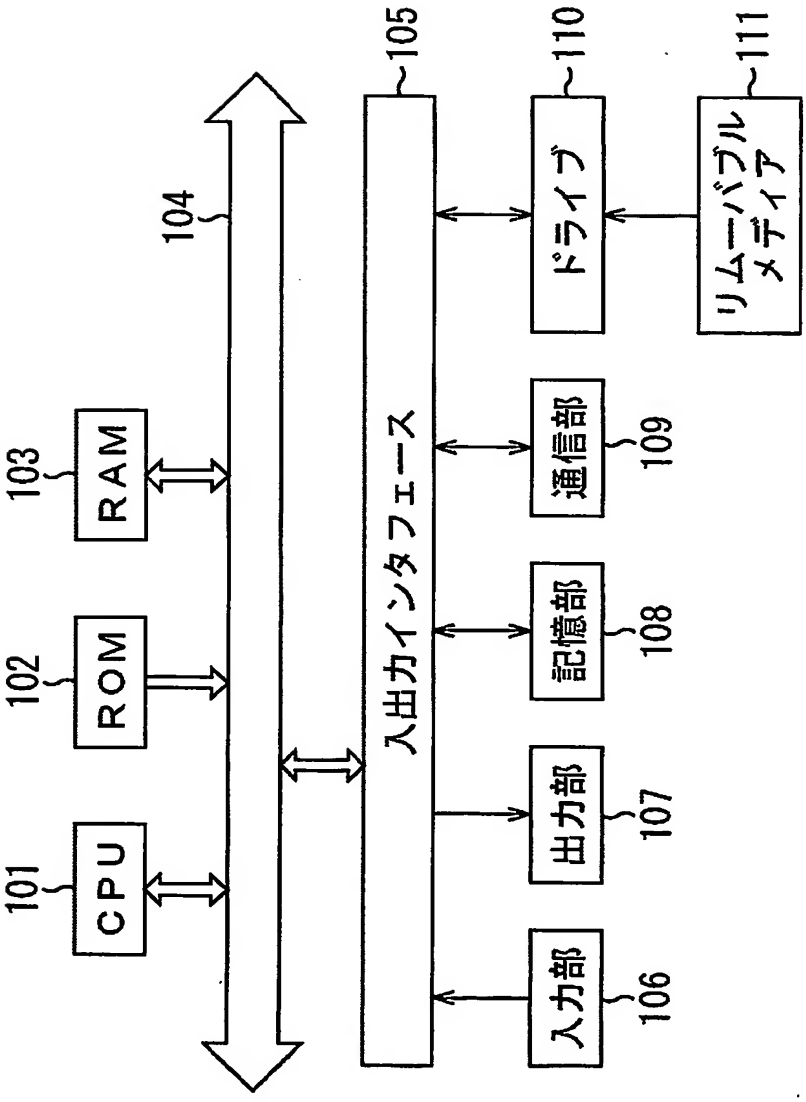
【書類名】図面
【図１】

図1



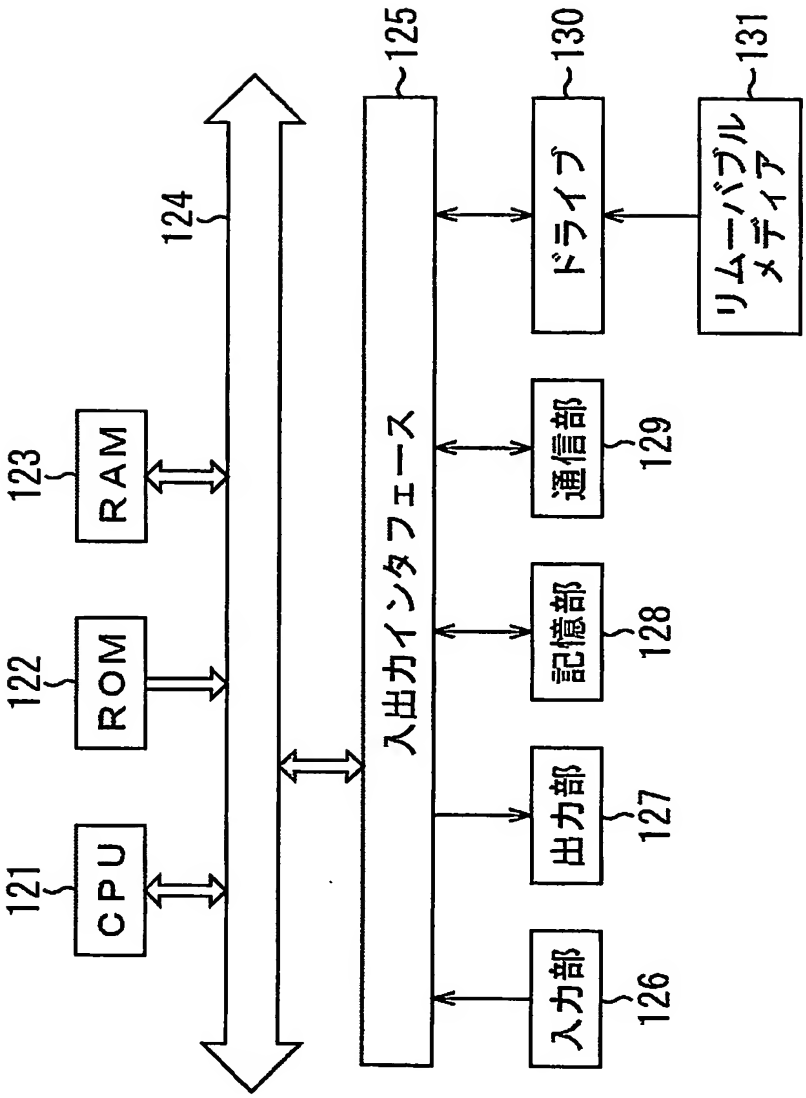
【図２】

図2


101
CPU
102
ROM
103
RAM
104
105
入出力インタフェース
106
入力部
107
出力部
108
記憶部
109
通信部
110
ドライブ
111
リムーバブル
メディア

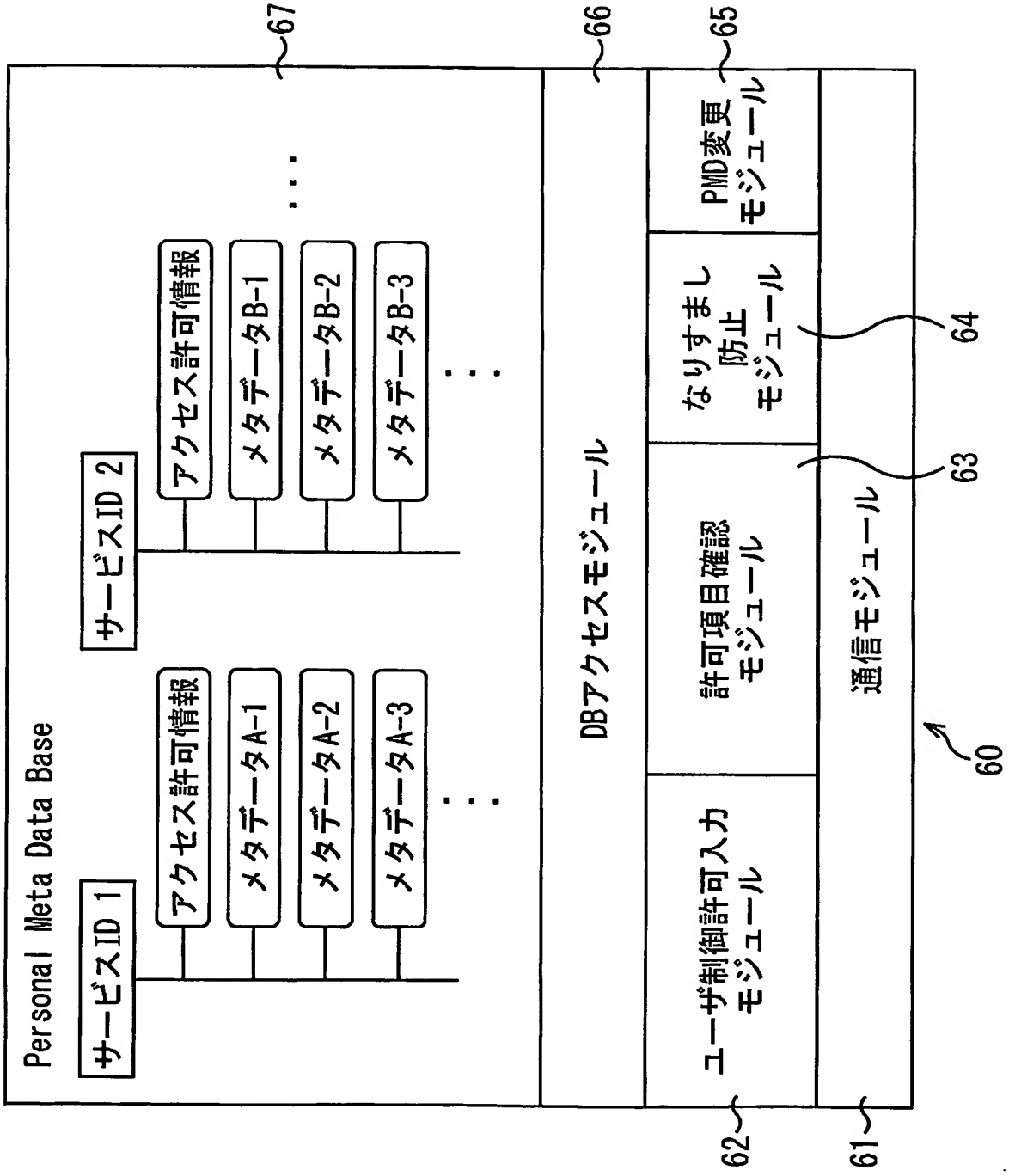
【図３】

図3


CPU
121
ROM
122
RAM
123
124
入出力インタフェース
125
入力部
126
出力部
127
記憶部
128
通信部
129
ドライブ
130
リムーバブル
メディア
131

【図４】

図4


Personal Meta Data Base
サービスID 1
アクセス許可情報
メタデータA-1
メタデータA-2
メタデータA-3
サービスID 2
アクセス許可情報
メタデータB-1
メタデータB-2
メタデータB-3
67
DBアクセスモジュール
66
ユーザ制御許可入力モジュール
62
許可項目確認モジュール
63
通信モジュール
61
なりすまし防止モジュール
64
PMD変更モジュール
65
60

【図５】

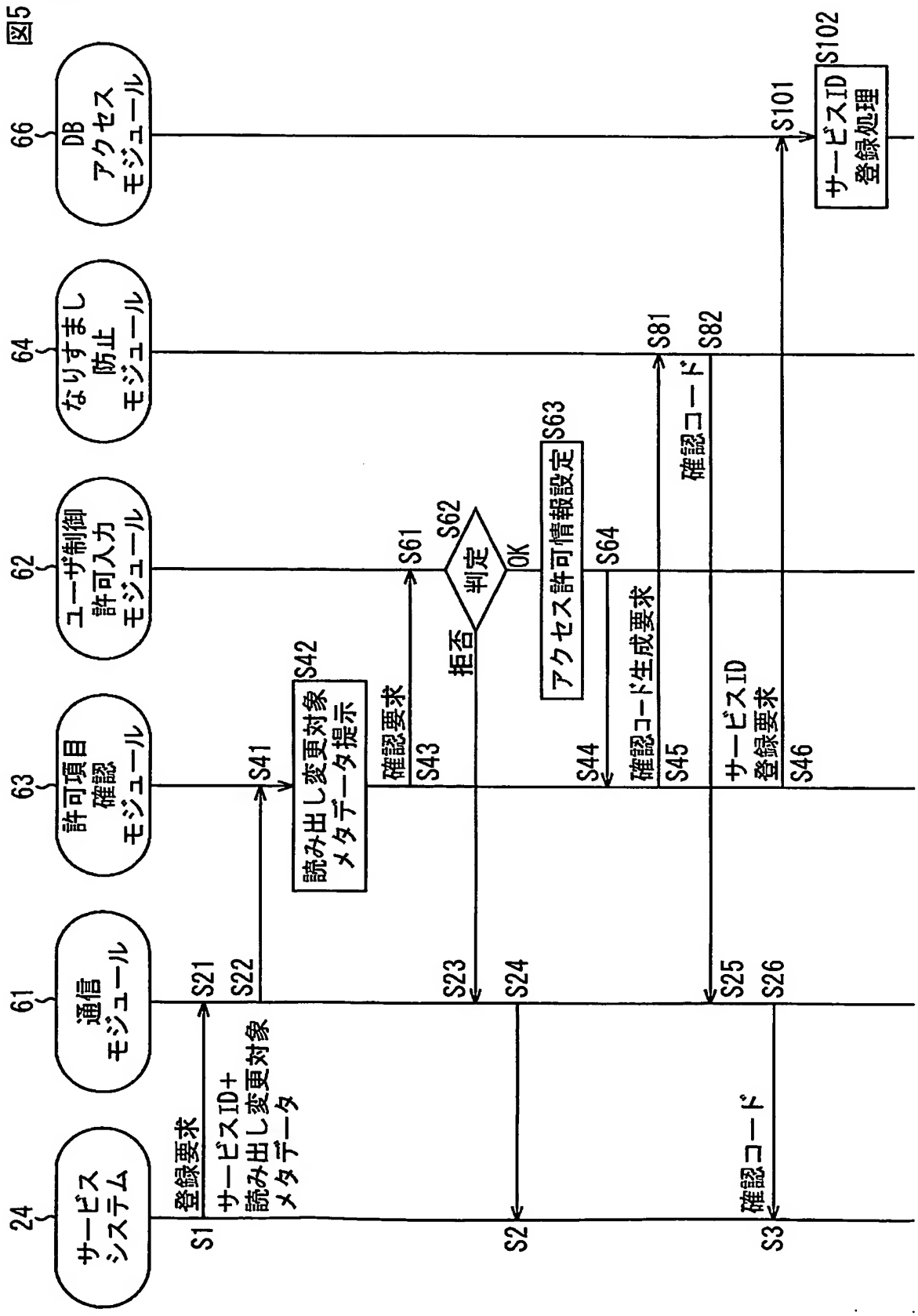


図5
24 サービスシステム
61 通信モジュール
63 許可項目確認モジュール
62 ユーザ制御許可入力モジュール
64 なりすまし防止モジュール
66 DBアクセスモジュール
登録要求
サービスID+読み出し変更対象メタデータ
読み出し変更対象メタデータ提示
確認要求
判定
拒否
OK
アクセス許可情報設定
確認コード生成要求
確認コード
サービスID登録要求
確認コード
サービスID登録処理
S1
S2
S3
S21
S22
S23
S24
S25
S26
S41
S42
S43
S44
S45
S46
S61
S62
S63
S64
S81
S82
S101
S102

【図６】

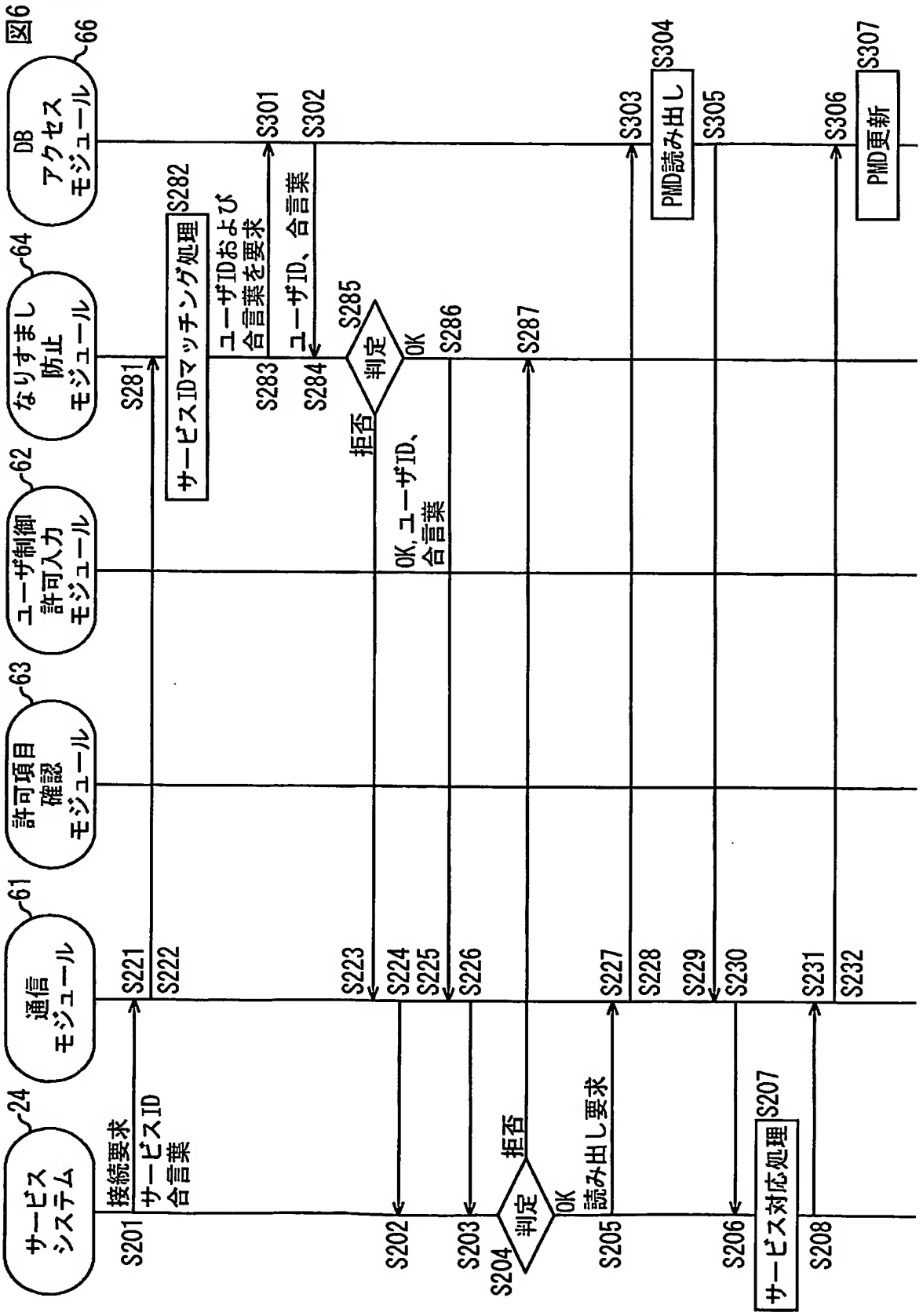
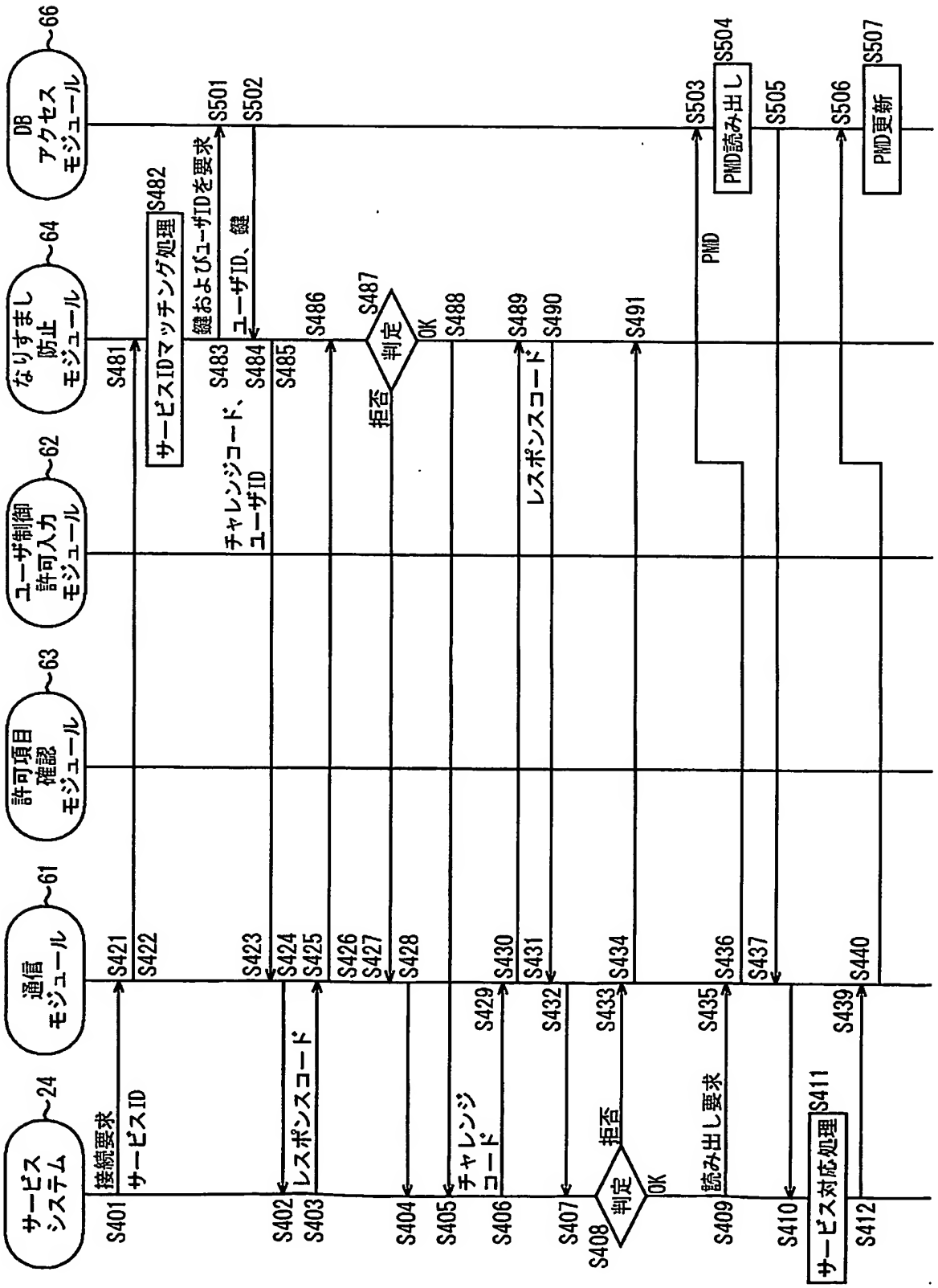


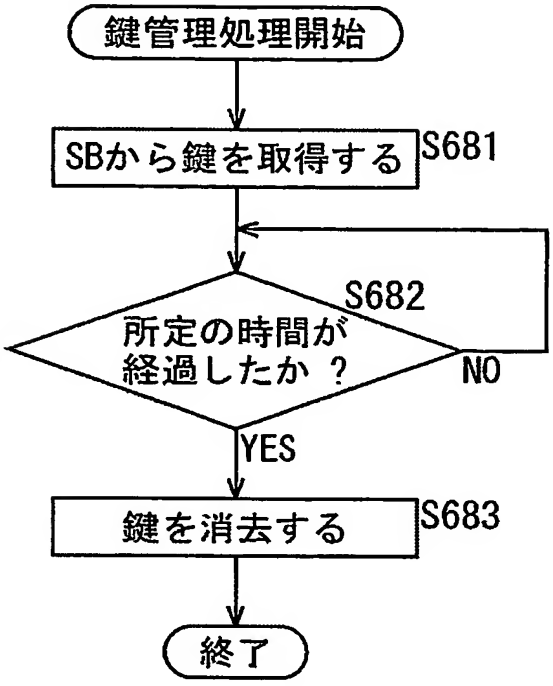
図6
サービスシステム 24
通信モジュール 61
許可項目確認モジュール 63
ユーザ制御許可入力モジュール 62
なりすまし防止モジュール 64
DBアクセスモジュール 66
接続要求
サービスID
合言葉
S201
S221
S222
S202
S223
S224
S225
S203
S226
判定
拒否
OK
S204
S227
S228
S205
読み出し要求
S229
S230
S206
S207
サービス対応処理
S231
S232
S208
サービスIDマッチング処理
S281
S282
ユーザIDおよび合言葉を要求
S283
S301
S284
S302
ユーザID、合言葉
S285
判定
拒否
OK
OK,ユーザID、合言葉
S286
S287
S303
PMD読み出し
S304
S305
S306
PMD更新
S307

【図７】

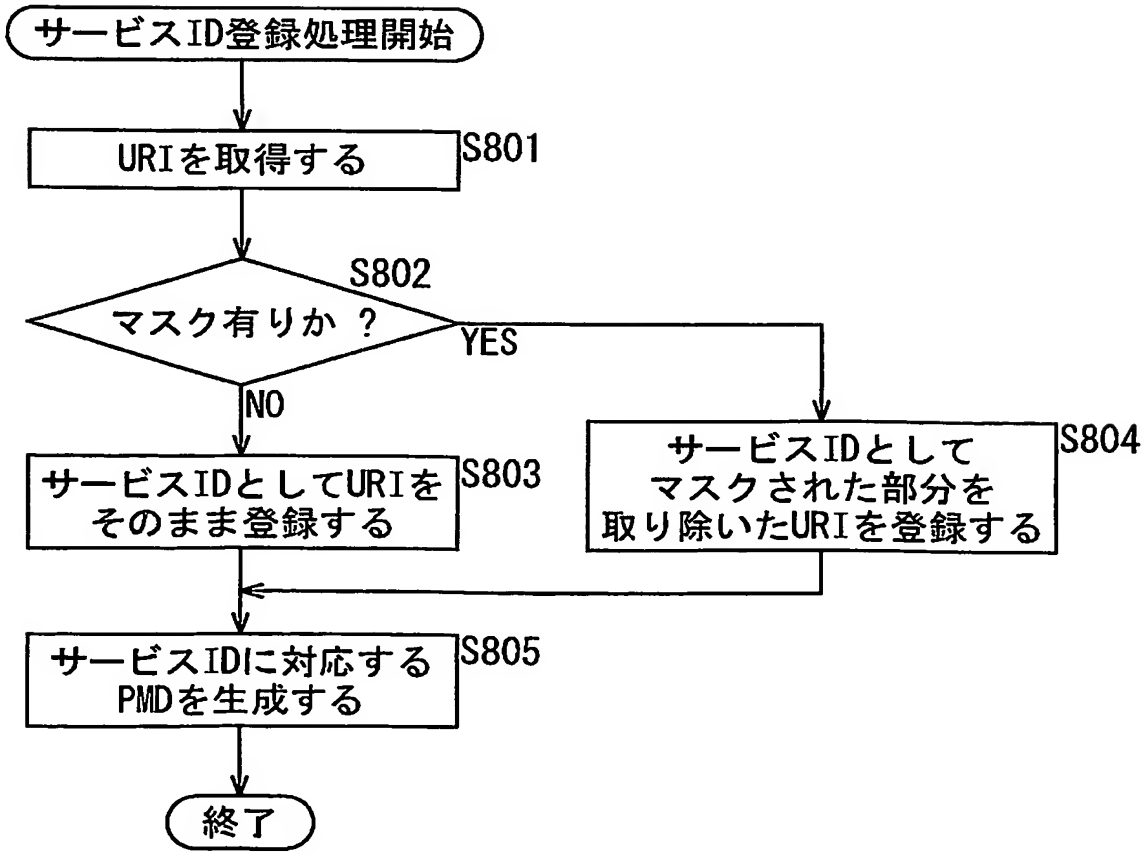
図7


サービスシステム
~24
通信モジュール
~61
許可項目確認モジュール
~63
ユーザ制御許可入力モジュール
~62
なりすまし防止モジュール
~64
DBアクセスモジュール
~66
S401 接続要求
S402 サービスID
S403 レスポンスコード
S404 チャレンジコード
S405
S406 判定 拒否
S407 OK
S408
S409 読み出し要求
S410
S411 サービス対応処理
S412
S421
S422
S423 サービスIDマッチング処理
S424 チャレンジコード、ユーザID
S425
S426 鍵およびユーザID要求
S427 ユーザID、鍵
S428
S429
S430 判定 拒否
S431 OK
S432 レスポンスコード
S433
S434
S435 PMD
S436 PMD読み出し
S437
S439
S440 PMD更新
S481
S482
S483
S484
S485
S486
S487
S488
S489
S490
S491
S501
S502
S503
S504
S505
S506
S507

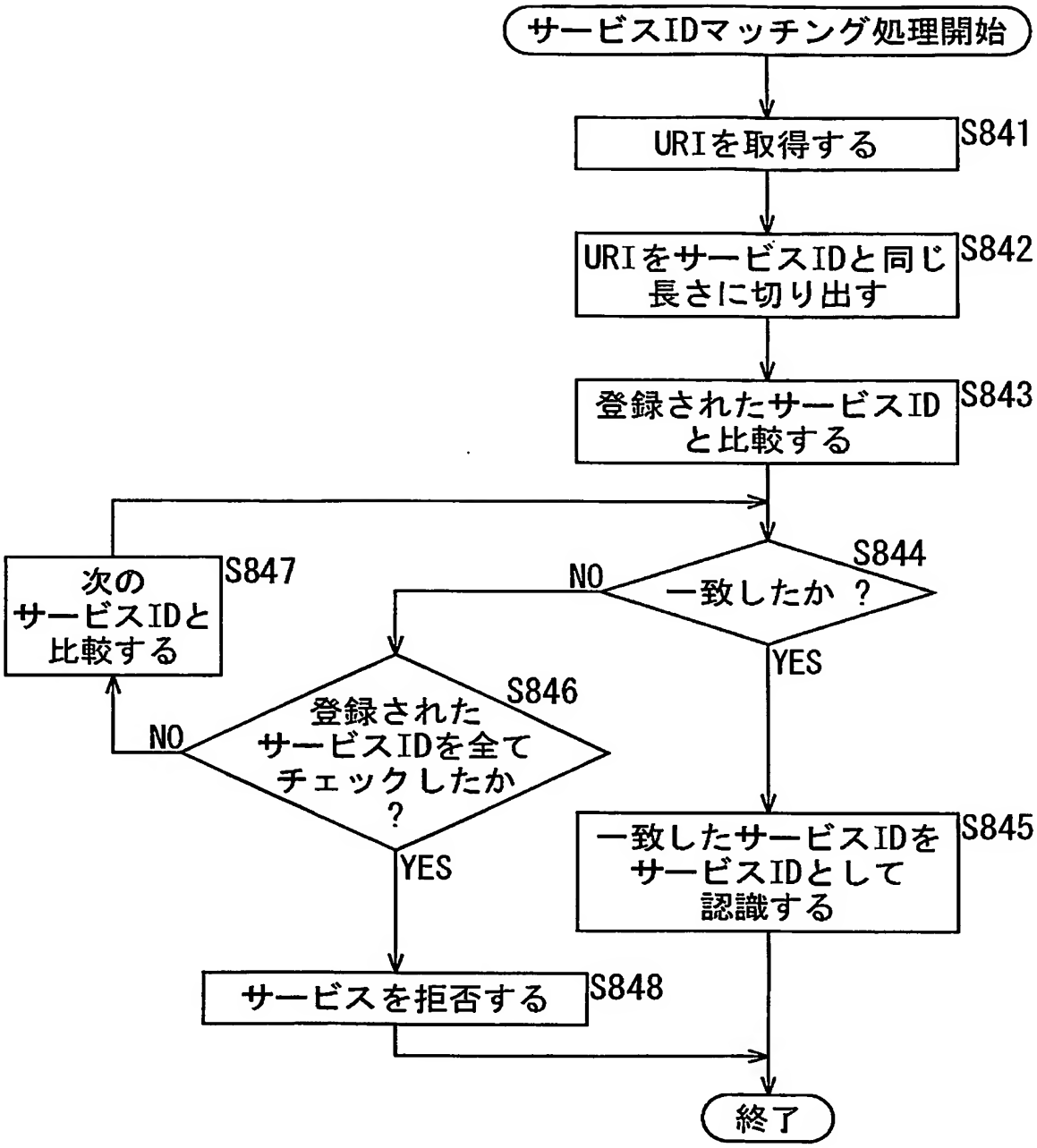
【図８】
図8


鍵管理処理開始
SBから鍵を取得する
S681
S682
所定の時間が
経過したか ？
NO
YES
鍵を消去する
S683
終了

【図９】
図9

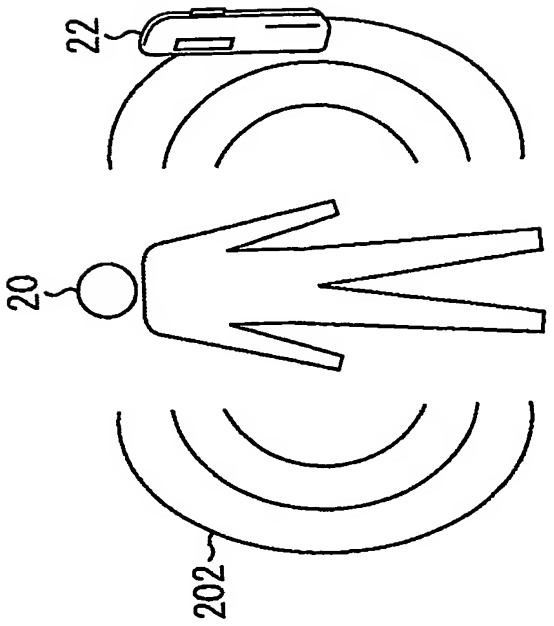

サービスID登録処理開始
URIを取得する
S801
S802
マスク有りか ？
YES
NO
サービスIDとしてURIを
そのまま登録する
S803
サービスIDとして
マスクされた部分を
取り除いたURIを登録する
S804
サービスIDに対応する
PMDを生成する
S805
終了

【図１０】
図10

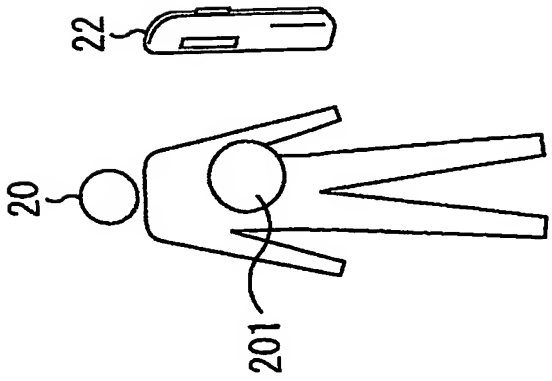

サービスIDマッチング処理開始
URIを取得する
S841
URIをサービスIDと同じ長さに切り出す
S842
登録されたサービスIDと比較する
S843
S844
一致したか ？
NO
YES
次のサービスIDと比較する
S847
登録されたサービスIDを全てチェックしたか ？
S846
NO
YES
一致したサービスIDをサービスIDとして認識する
S845
サービスを拒否する
S848
終了

【図１１】

図11

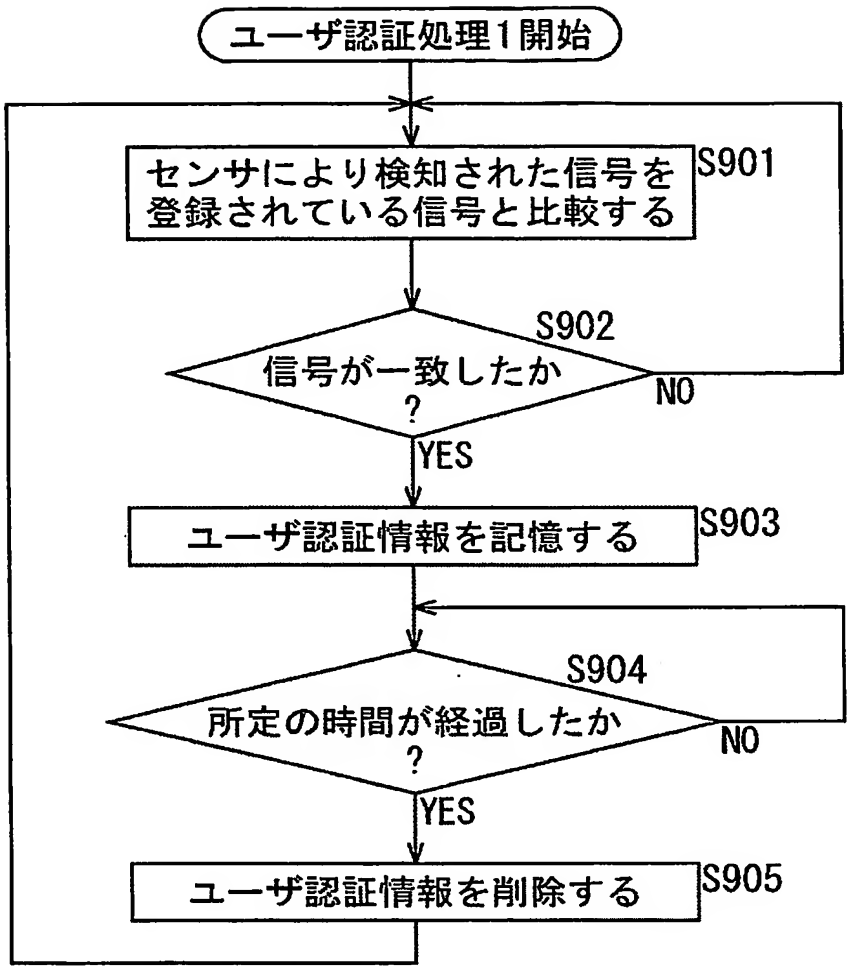


B

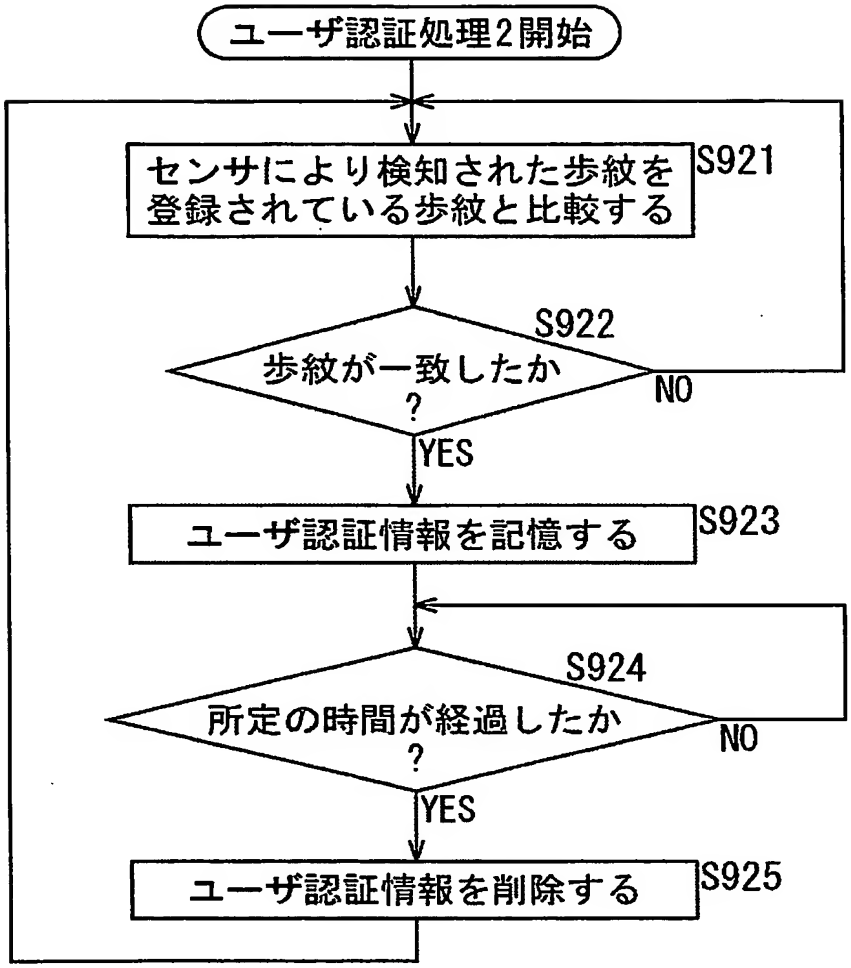


A

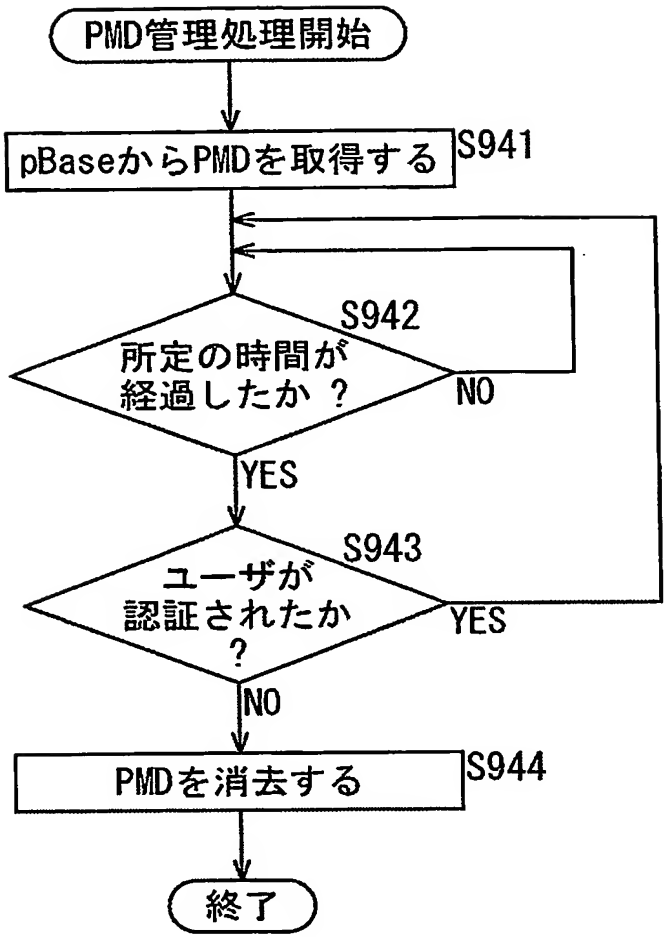
【図１２】
図12


ユーザ認証処理１開始
センサにより検知された信号を登録されている信号と比較する
S901
S902
信号が一致したか？
NO
YES
ユーザ認証情報を記憶する
S903
S904
所定の時間が経過したか？
NO
YES
ユーザ認証情報を削除する
S905

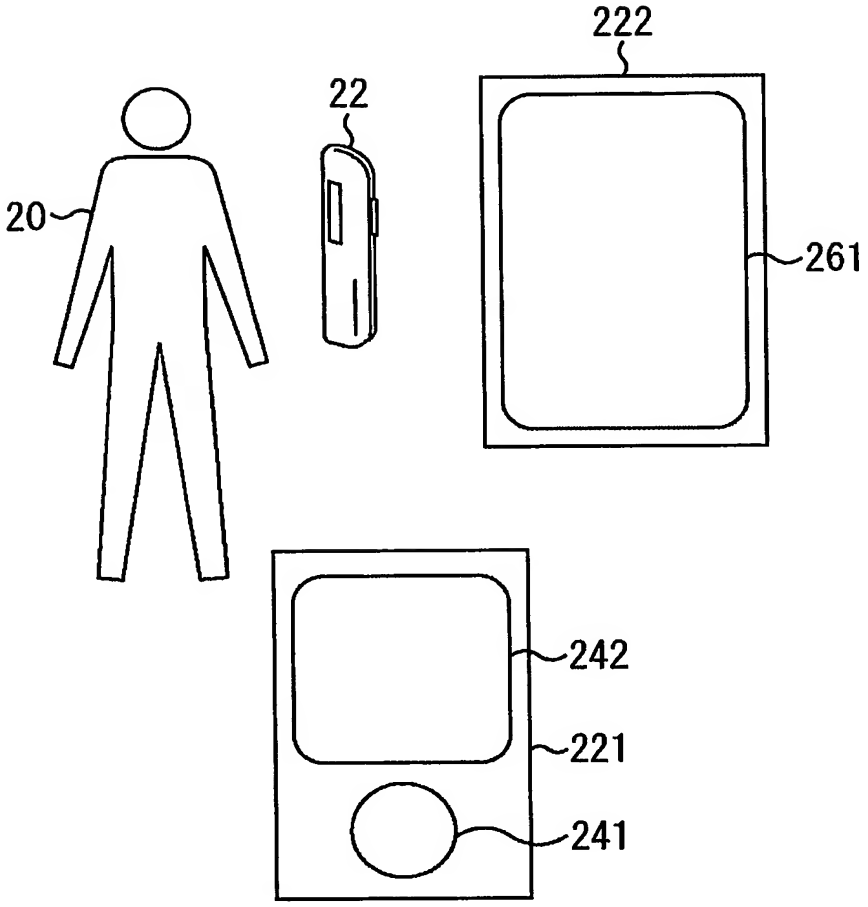
【図１３】
図13


ユーザ認証処理2開始
センサにより検知された歩紋を登録されている歩紋と比較する
S921
S922
歩紋が一致したか？
NO
YES
ユーザ認証情報を記憶する
S923
S924
所定の時間が経過したか？
NO
YES
ユーザ認証情報を削除する
S925

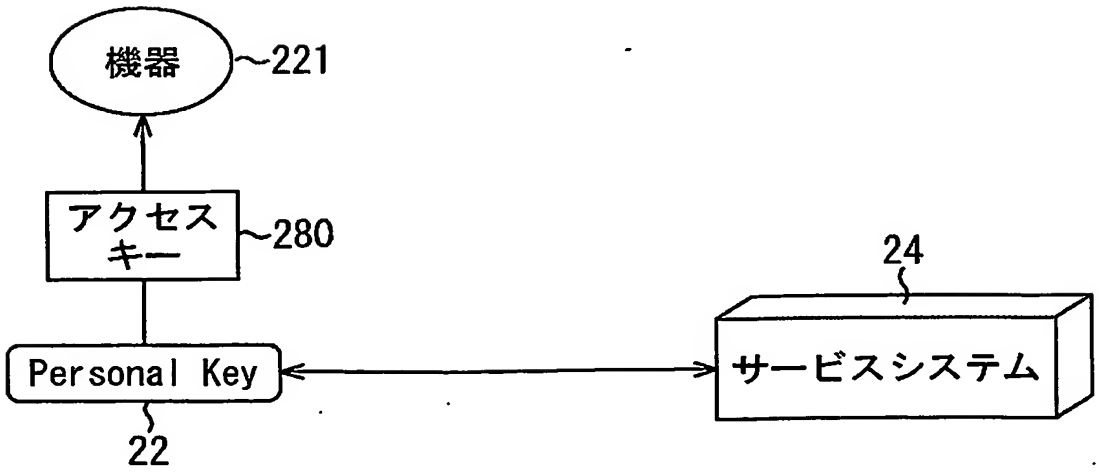
【図１４】
図14


PMD管理処理開始
pBaseからPMDを取得する
S941
S942
所定の時間が
経過したか ？
NO
YES
S943
ユーザが
認証されたか
？
YES
NO
PMDを消去する
S944
終了

【図１５】
図15

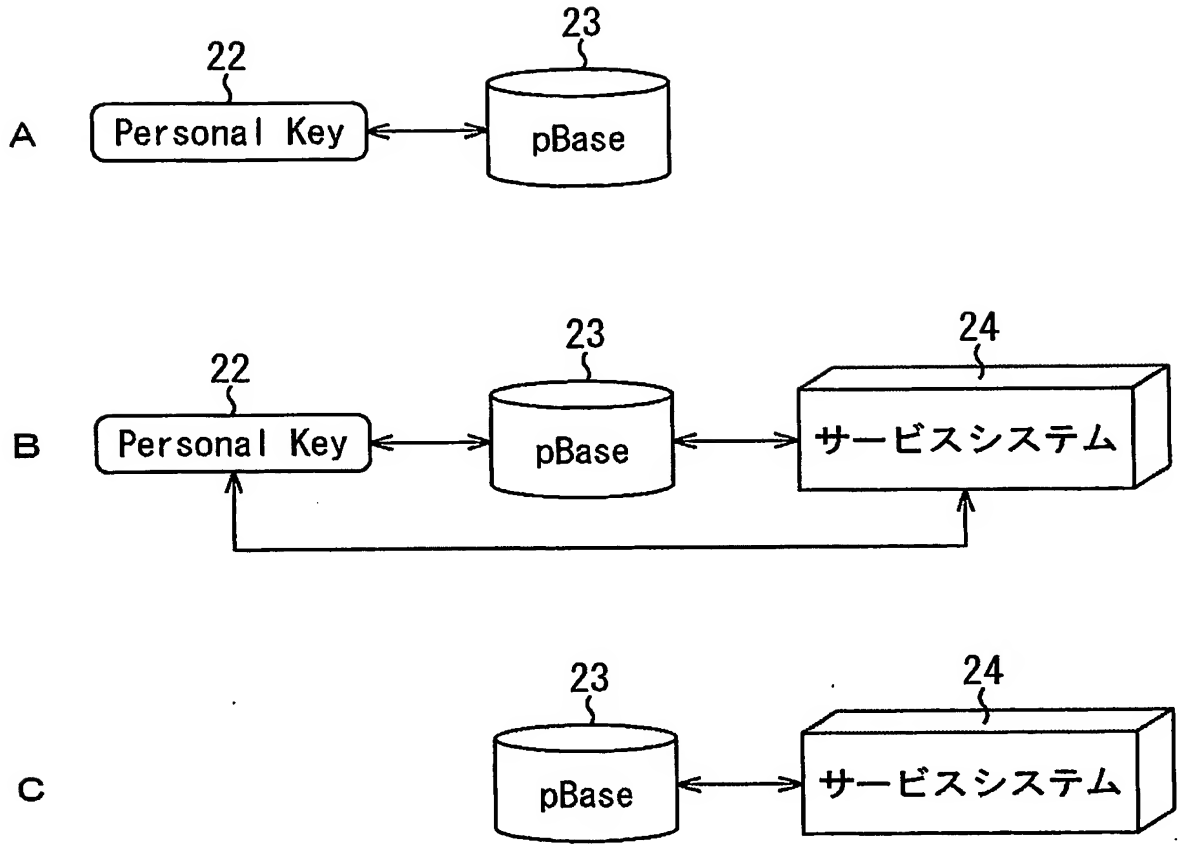


【図１６】
図16



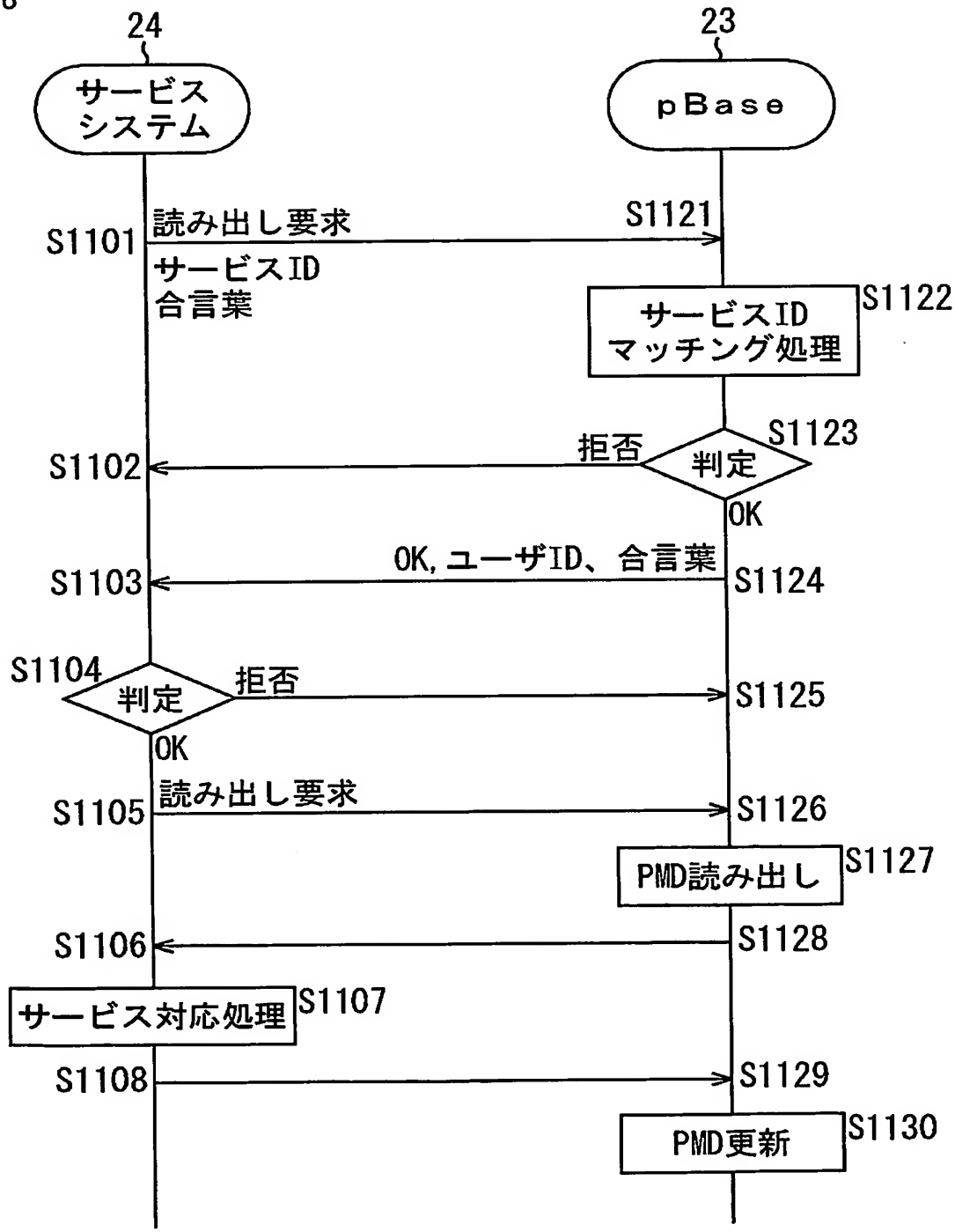
【図１７】

図17


A
22
Personal Key
23
pBase
B
22
Personal Key
23
pBase
24
サービスシステム
C
23
pBase
24
サービスシステム

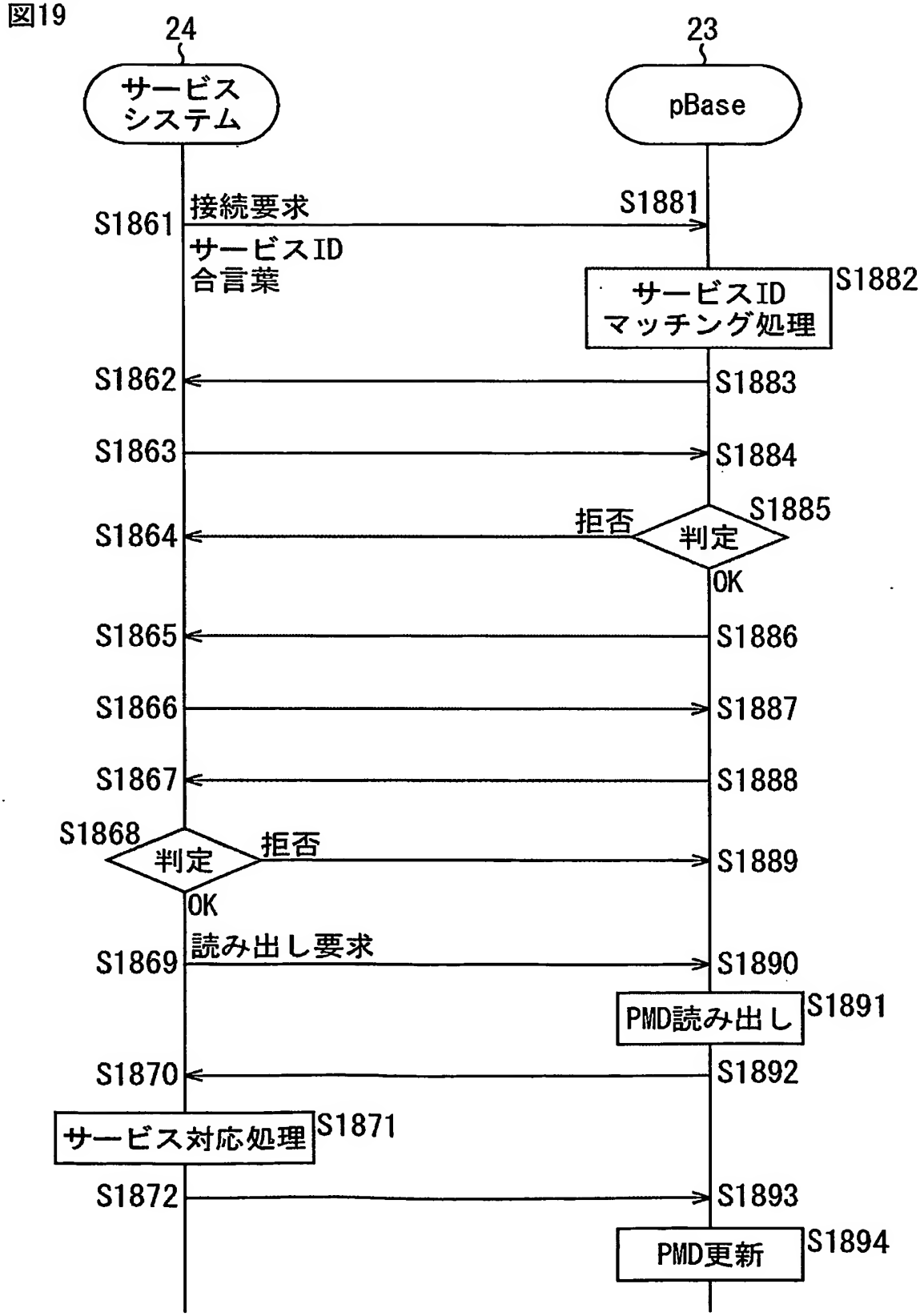
【図１８】

図18


24
サービス
システム
23
pBase
S1101
読み出し要求
サービスID
合言葉
S1121
S1122
サービスID
マッチング処理
S1123
判定
拒否
S1102
OK
OK, ユーザID、合言葉
S1103
S1124
S1104
判定
拒否
S1125
OK
S1105
読み出し要求
S1126
PMD読み出し
S1127
S1106
S1128
サービス対応処理
S1107
S1108
S1129
PMD更新
S1130

【図１９】

図19


24
23
サービス
システム
pBase
S1861
接続要求
サービスID
合言葉
S1881
サービスID
マッチング処理
S1882
S1862
S1883
S1863
S1884
S1864
拒否
判定
S1885
OK
S1865
S1886
S1866
S1887
S1867
S1888
S1868
判定
拒否
S1889
OK
S1869
読み出し要求
S1890
PMD読み出し
S1891
S1870
S1892
サービス対応処理
S1871
S1872
S1893
PMD更新
S1894

【図２０Ａ】

図20A

プロパティ	内容	アクセス制御
name	foo	制御情報
なりすまし防止方法	公開鍵方式	制御情報
サービス公開鍵	鍵データ	制御情報
PK秘密鍵	鍵データ	制御情報
action	プログラム	制御情報
番組嗜好情報	スポーツ10 バラエティ7 音楽5 その他3	制御情報

・
・
・

【図２０Ｂ】

図20B

プロパティ	内容	アクセス制御
name	foo	制御情報
なりすまし防止方法	共通鍵方式	制御情報
共通鍵	鍵データ	制御情報
action	プログラム	制御情報
番組嗜好情報	スポーツ10 バラエティ7 音楽5 その他3	制御情報

：
：

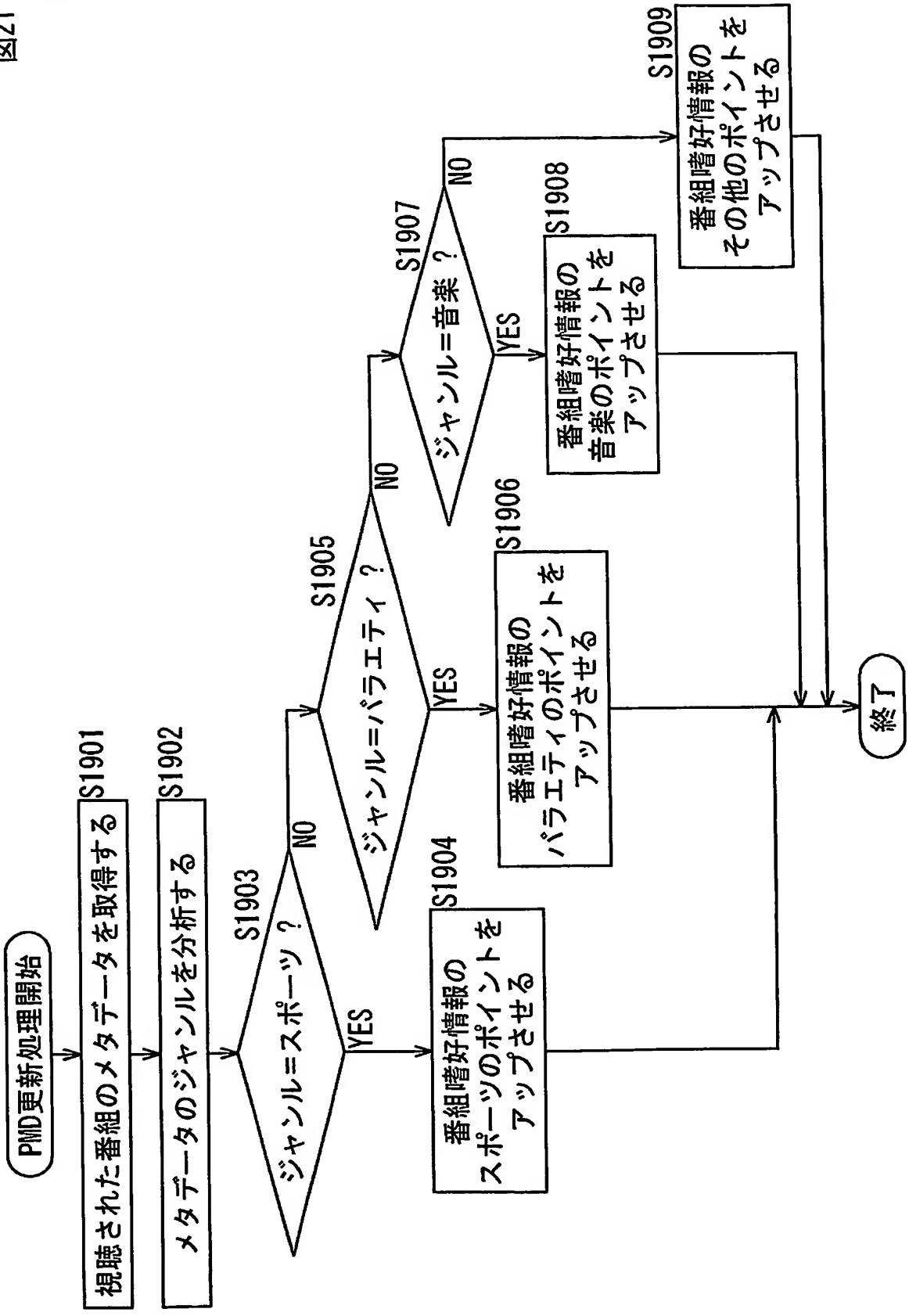
【図２０Ｃ】

図20C

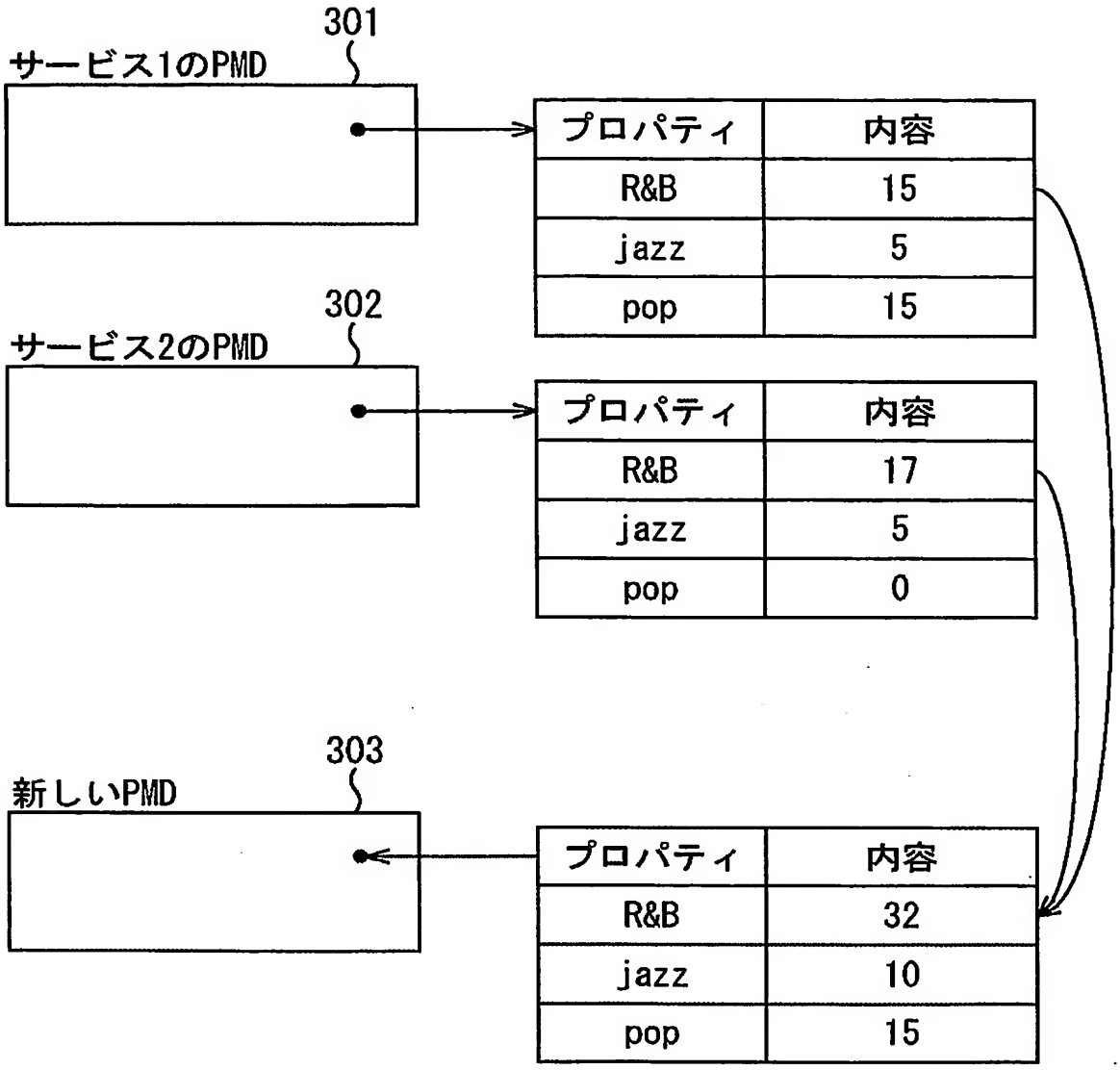
プロパティ	内容	アクセス制御
name	foo	制御情報
なりすまし防止方法	合言葉方式	制御情報
サービス合言葉	合言葉データ	制御情報
PK合言葉	合言葉データ	制御情報
action	プログラム	制御情報
番組嗜好情報	スポーツ10 バラエティ7 音楽5 その他3	制御情報
・	・	・
・	・	・
・	・	・

【図２１】

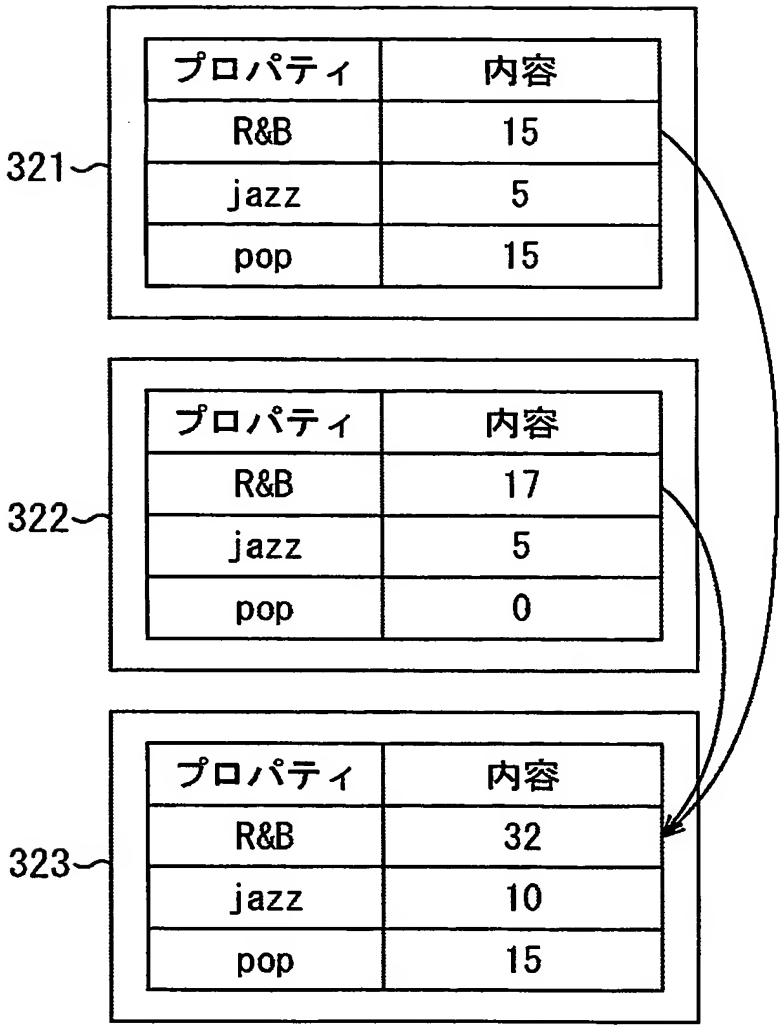
図21


PMD更新処理開始
S1901
視聴された番組のメタデータを取得する
S1902
メタデータのジャンルを分析する
S1903
ジャンル＝スポーツ？
YES
S1904
番組嗜好情報の
スポーツのポイントを
アップさせる
NO
S1905
ジャンル＝バラエティ？
YES
S1906
番組嗜好情報の
バラエティのポイントを
アップさせる
NO
S1907
ジャンル＝音楽？
YES
S1908
番組嗜好情報の
音楽のポイントを
アップさせる
NO
S1909
番組嗜好情報の
その他のポイントを
アップさせる
終了

【図２２】
図22

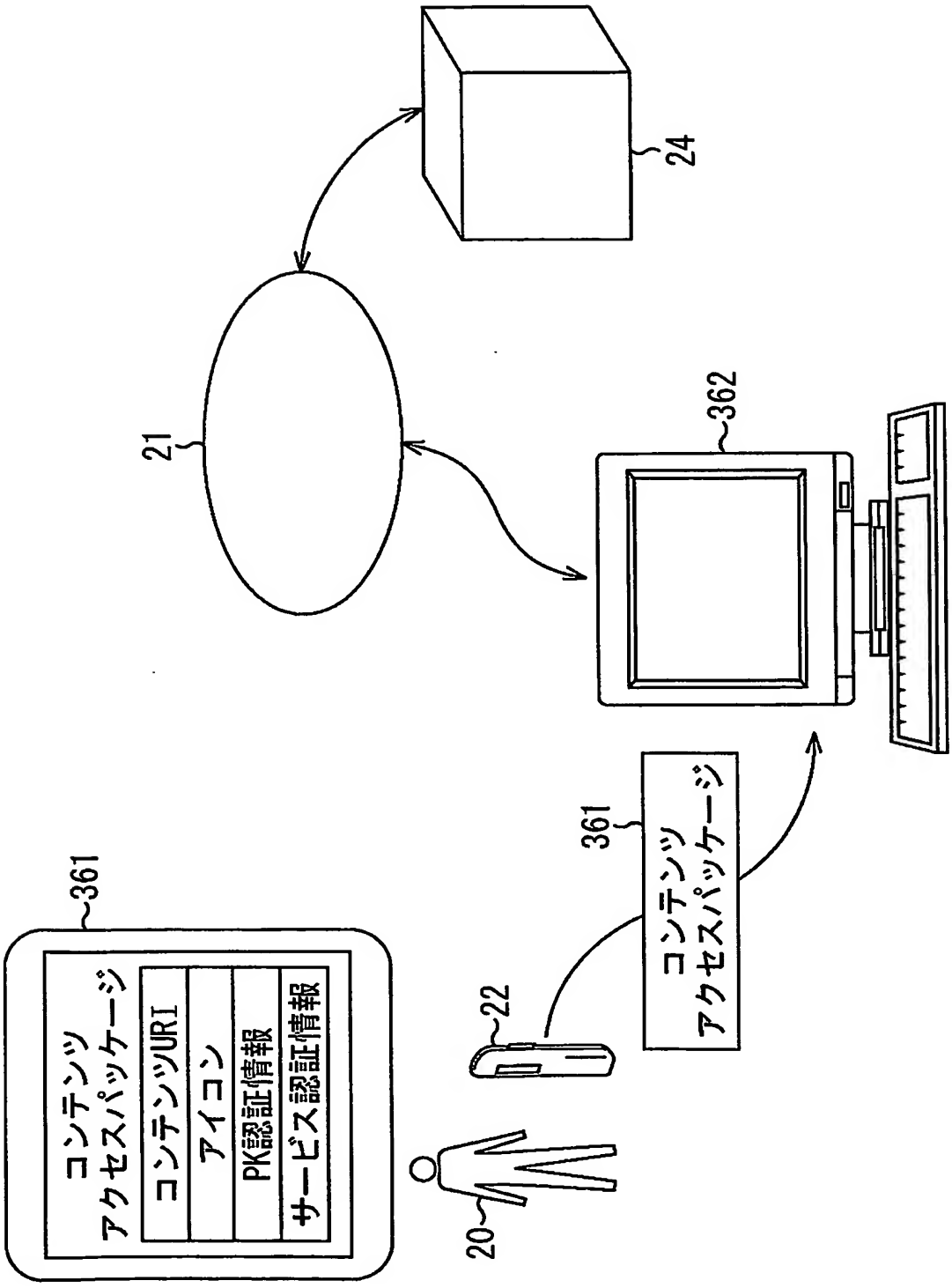

301
サービス1のPMD
プロパティ
内容
R&B
15
jazz
5
pop
15
302
サービス2のPMD
プロパティ
内容
R&B
17
jazz
5
pop
0
303
新しいPMD
プロパティ
内容
R&B
32
jazz
10
pop
15

【図２３】
図23


321
プロパティ
内容
R&B
15
jazz
5
pop
15
322
プロパティ
内容
R&B
17
jazz
5
pop
0
323
プロパティ
内容
R&B
32
jazz
10
pop
15

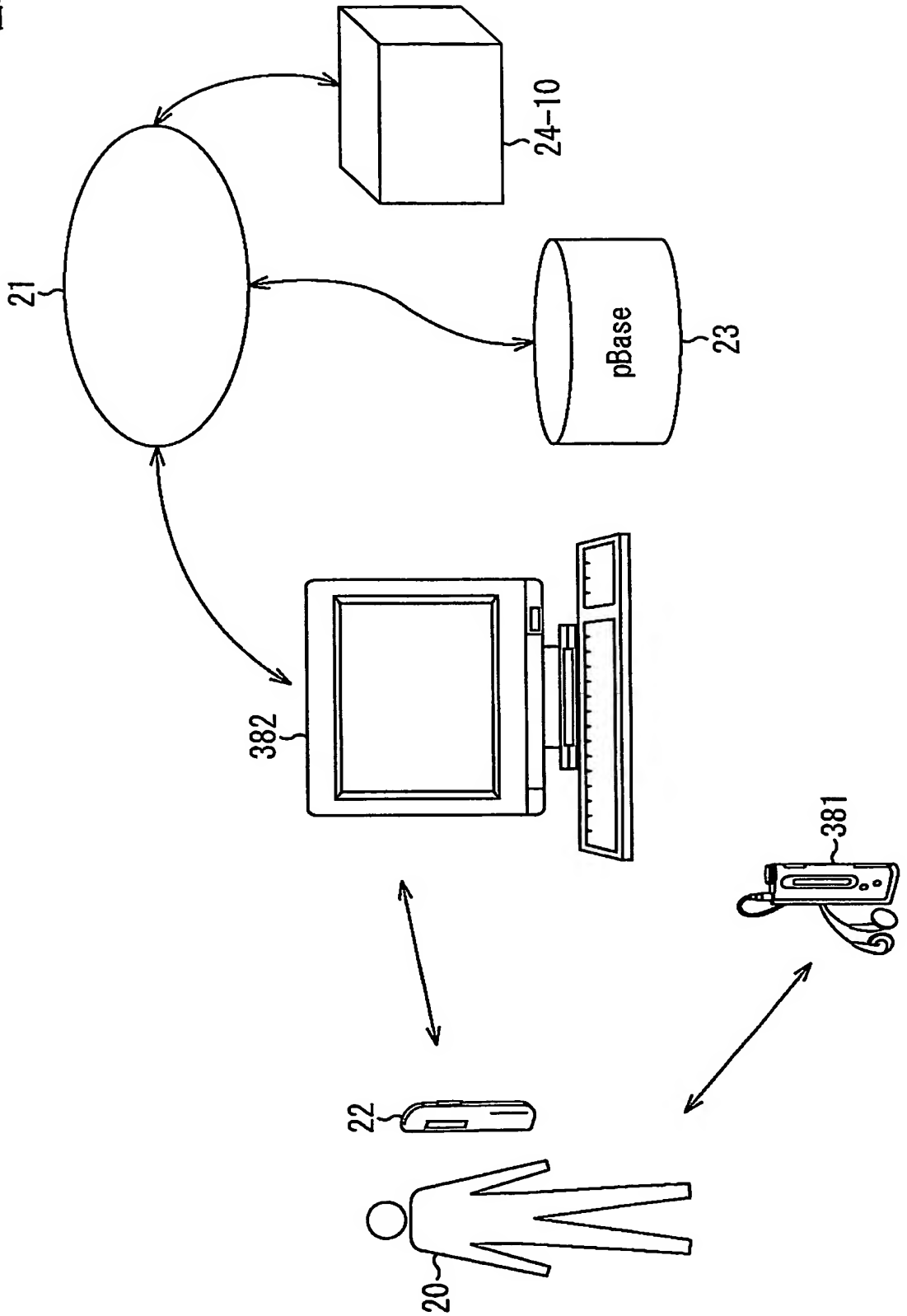
【図２４】

図24

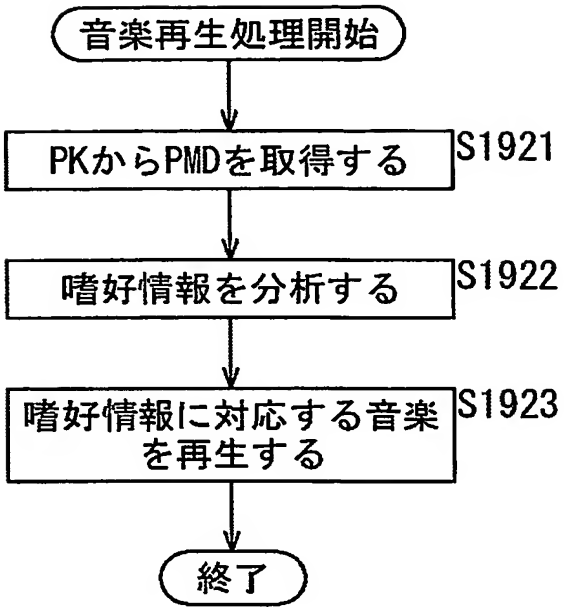

24
21
362
361
コンテンツ
アクセスパッケージ
361
コンテンツ
アクセスパッケージ
コンテンツURI
アイコン
PK認証情報
サービス認証情報
22
20

【図２５】

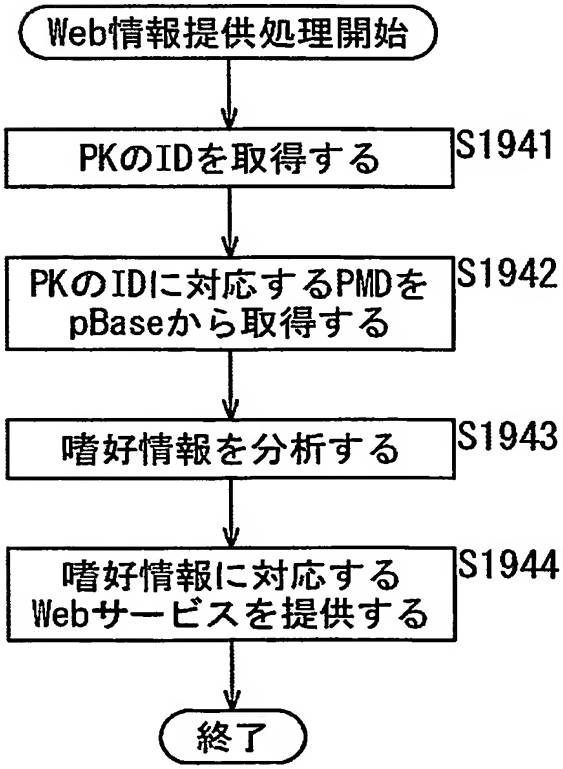
図25



【図２６】
図26

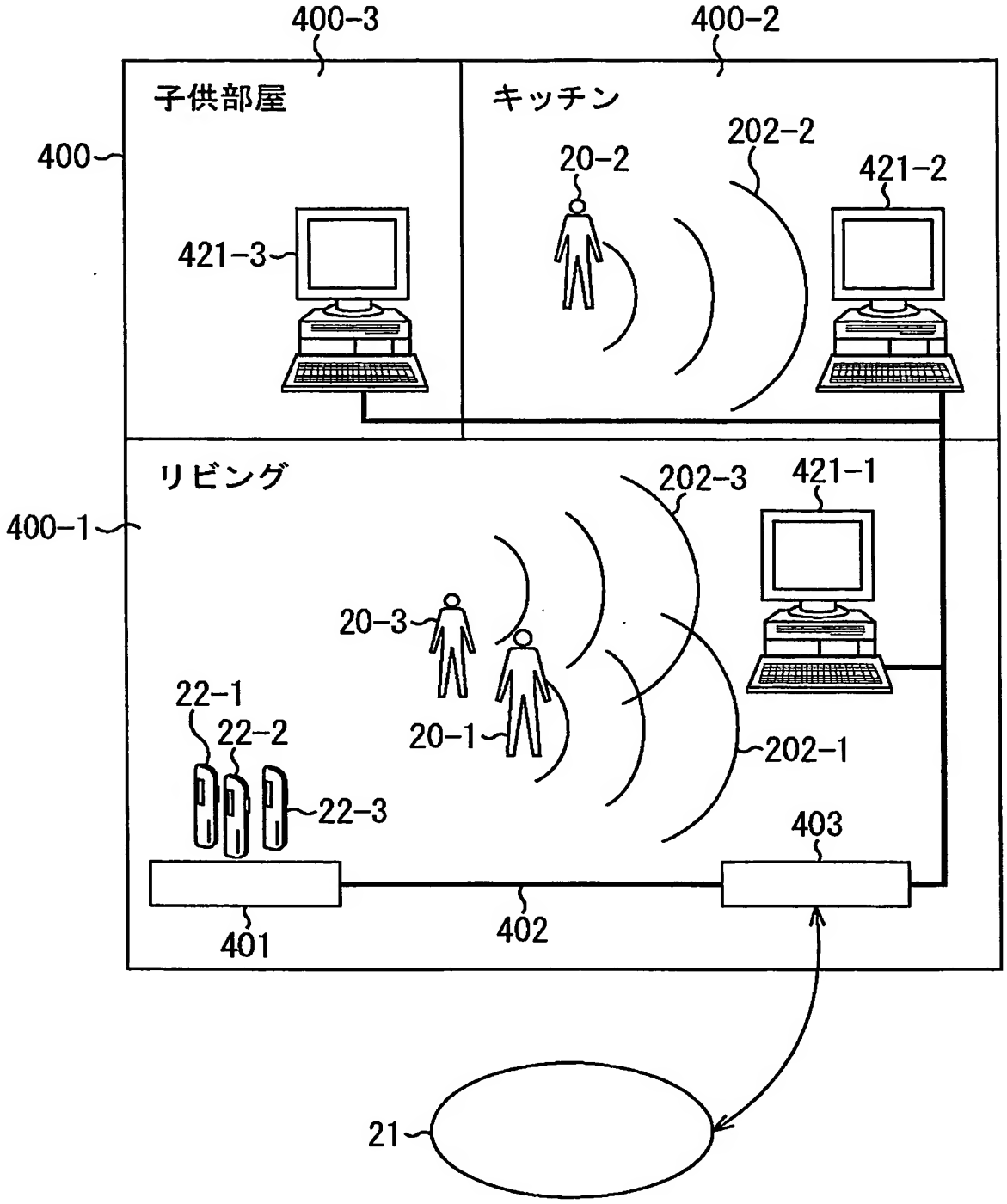


【図２７】
図27



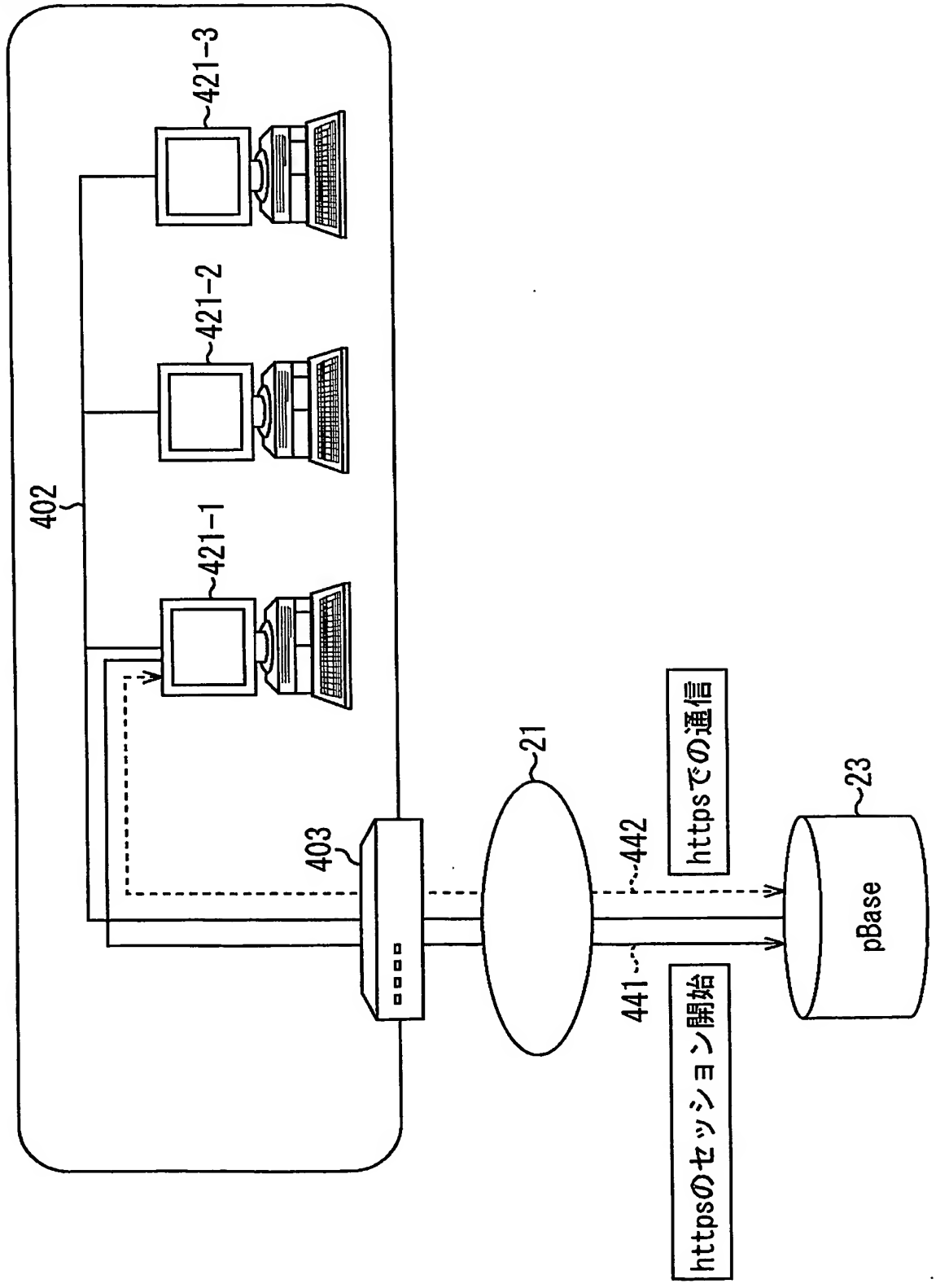
【図２８】

図28


400-3
400-2
子供部屋
キッチン
400
202-2
20-2
421-2
421-3
リビング
400-1
202-3
421-1
20-3
22-1
22-2
20-1
202-1
22-3
403
401
402
21

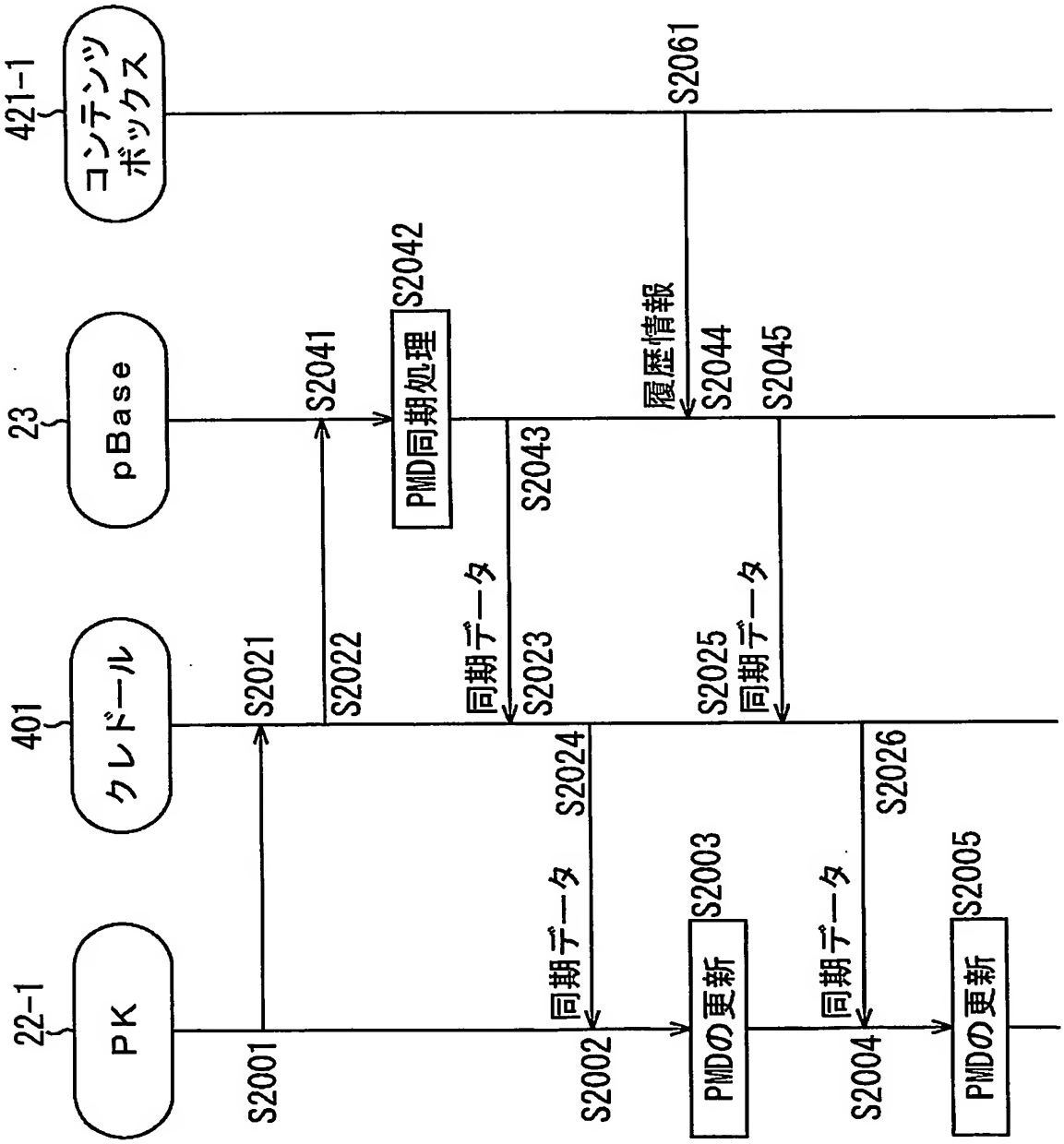
【図２９】

図29

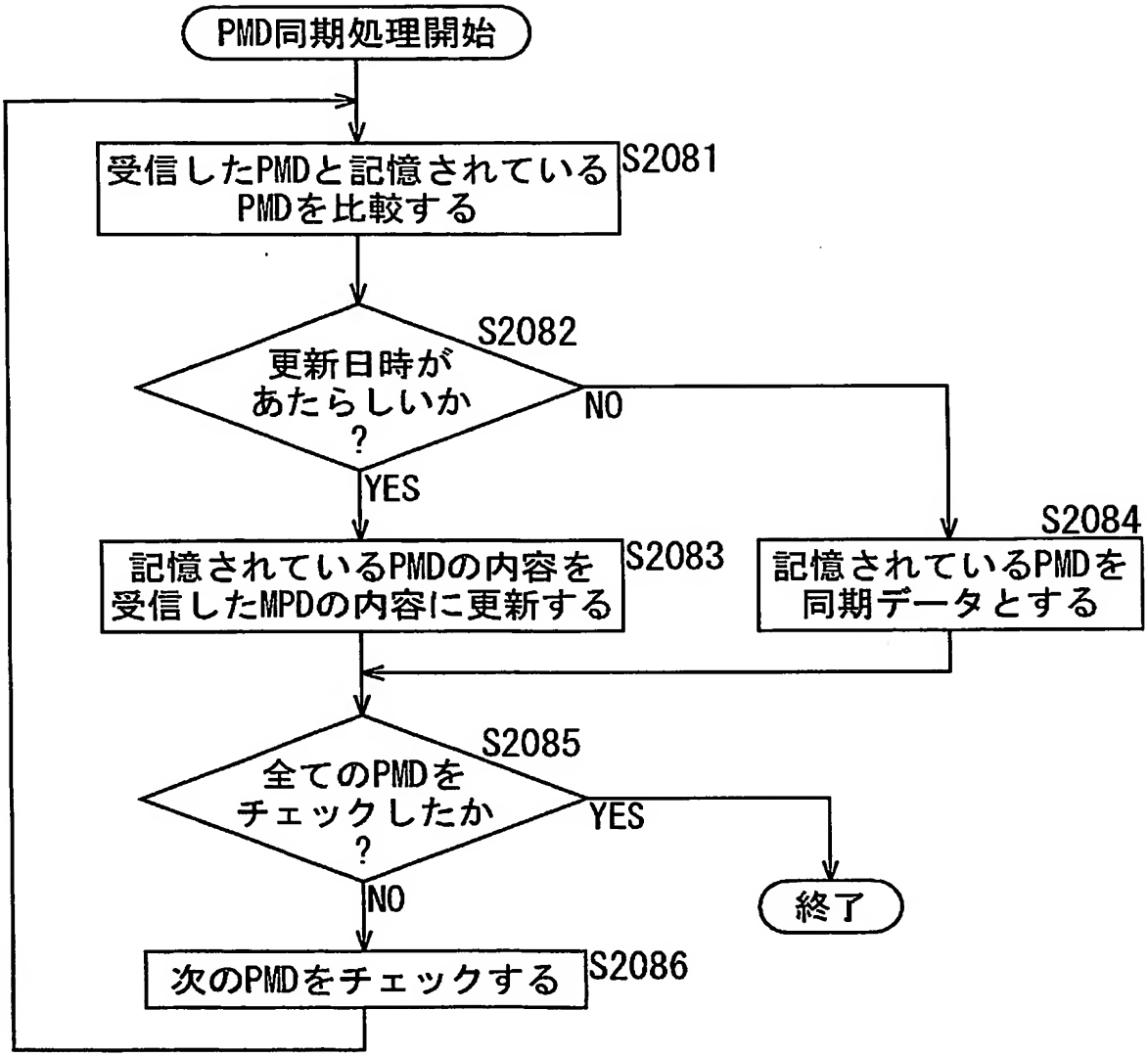

421-3
421-2
421-1
402
403
21
442
441
23
pBase
httpsでの通信
httpsのセッション開始

【図３０】

図30

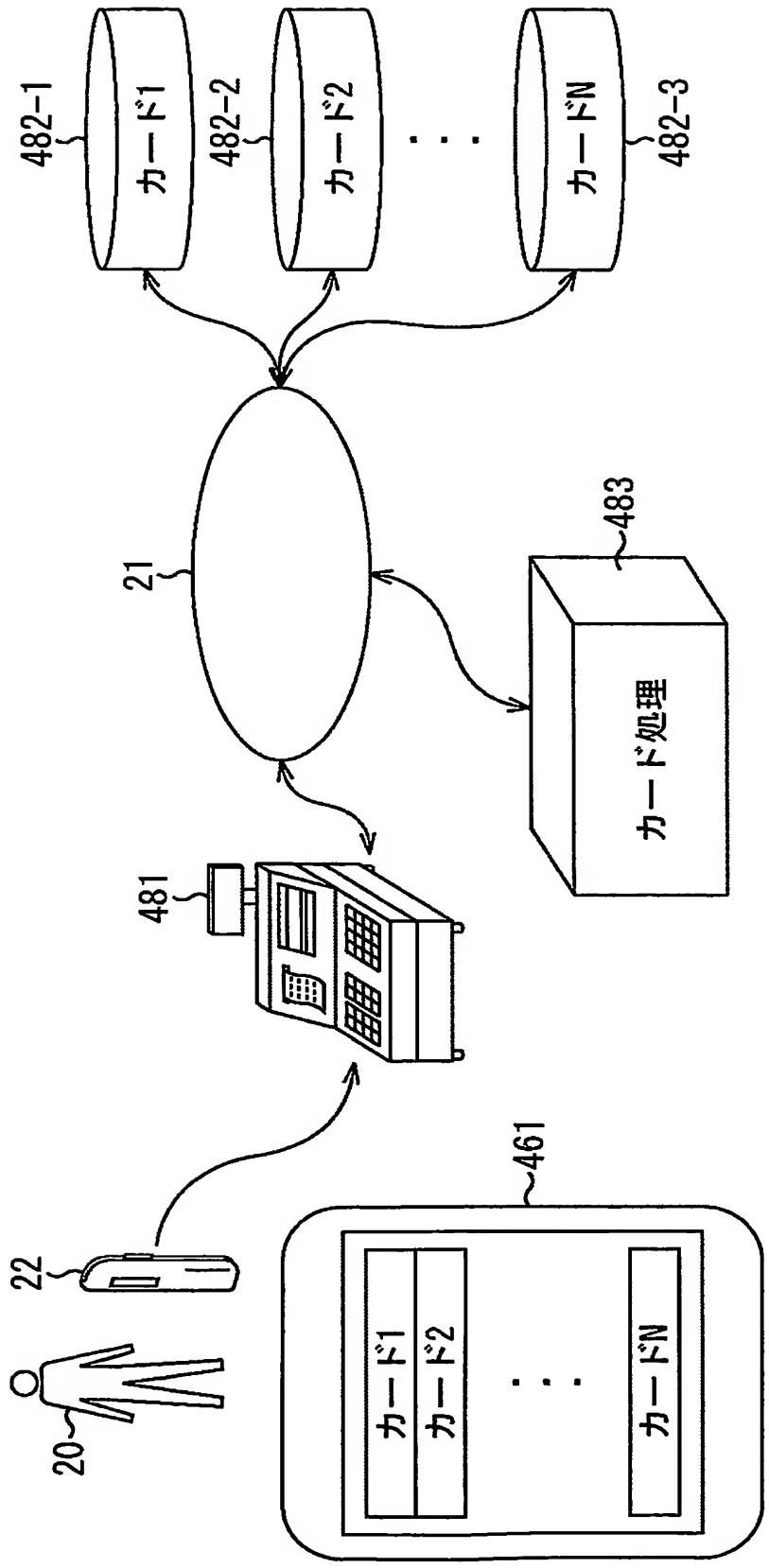

421-1
コンテンツボックス
23
pBase
401
クレドール
22-1
PK
S2001
S2002
S2003
S2004
S2005
S2021
S2022
S2023
S2024
S2025
S2026
S2041
S2042
S2043
S2044
S2045
S2061
PMD同期処理
履歴情報
同期データ
同期データ
同期データ
PMDの更新
PMDの更新

【図３１】
図31


PMD同期処理開始
受信したPMDと記憶されている
PMDを比較する
S2081
更新日時が
あたらしいか
？
S2082
NO
YES
記憶されているPMDの内容を
受信したMPDの内容に更新する
S2083
記憶されているPMDを
同期データとする
S2084
全てのPMDを
チェックしたか
？
S2085
YES
NO
終了
次のPMDをチェックする
S2086

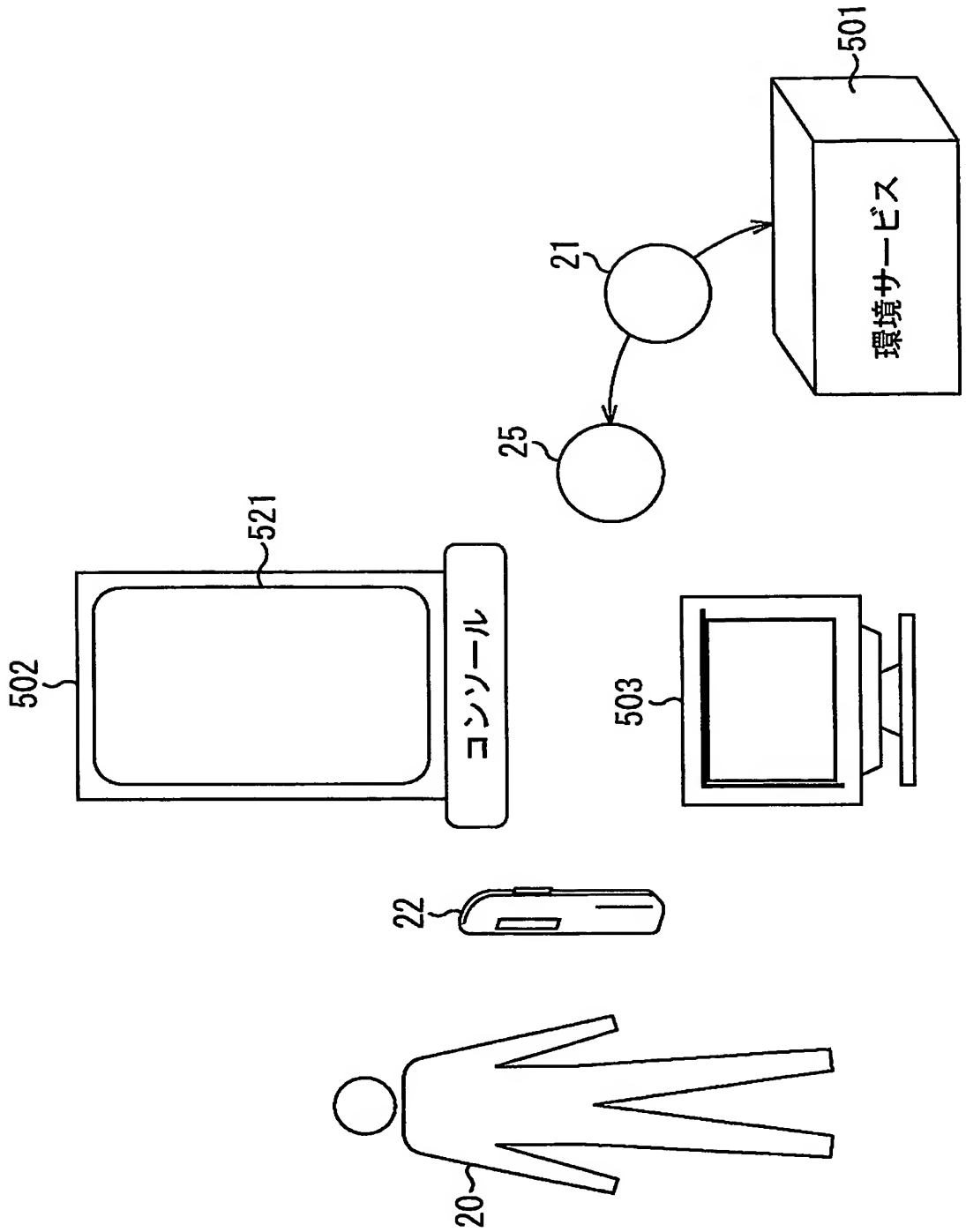
【図３２】

図32


482-1
カードｆ1
482-2
カードｆ2
・・・
カードｆN
482-3
21
483
カード処理
481
461
22
20
カードｆ1
カードｆ2
・・・
カードｆN

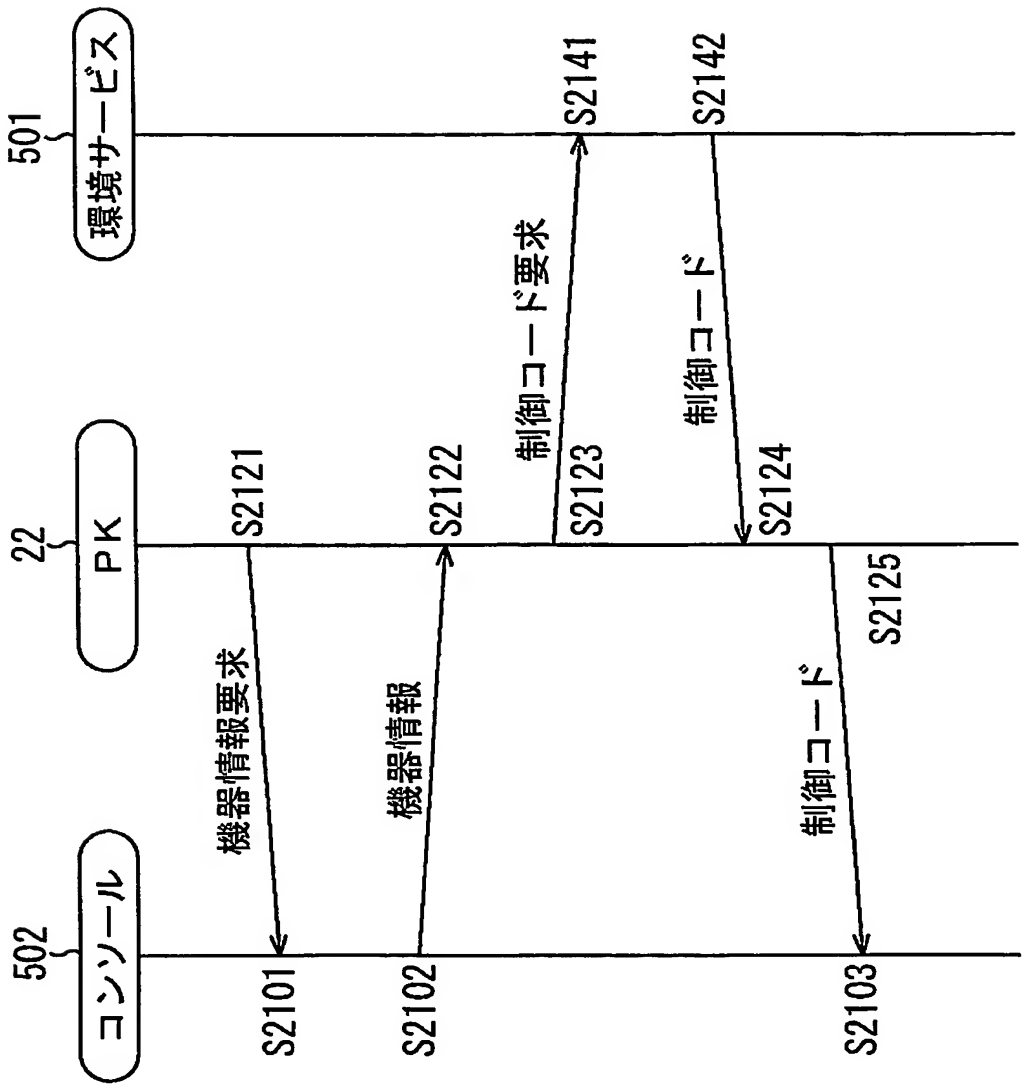
【図３３】

図33



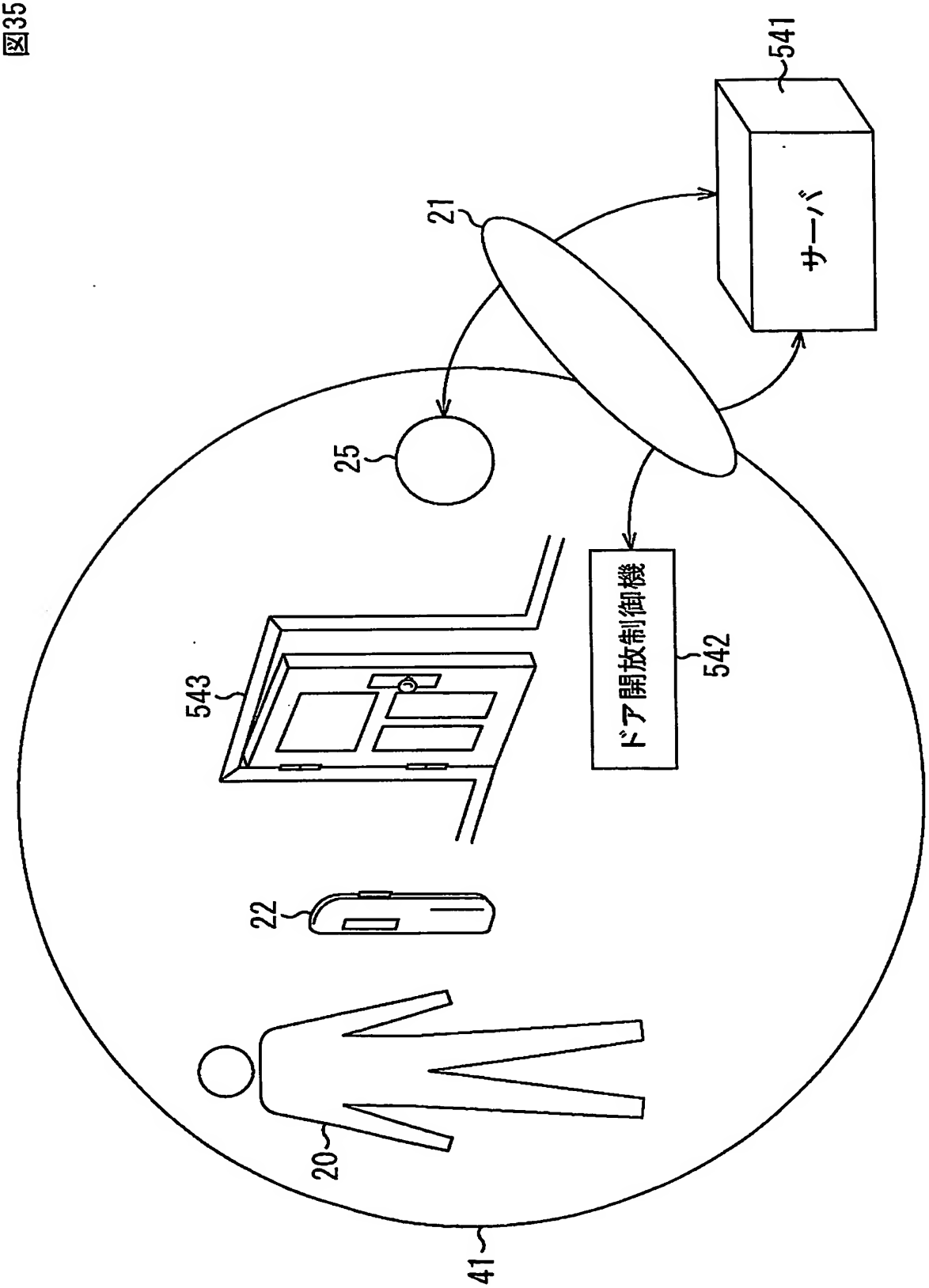
【図３４】

図34

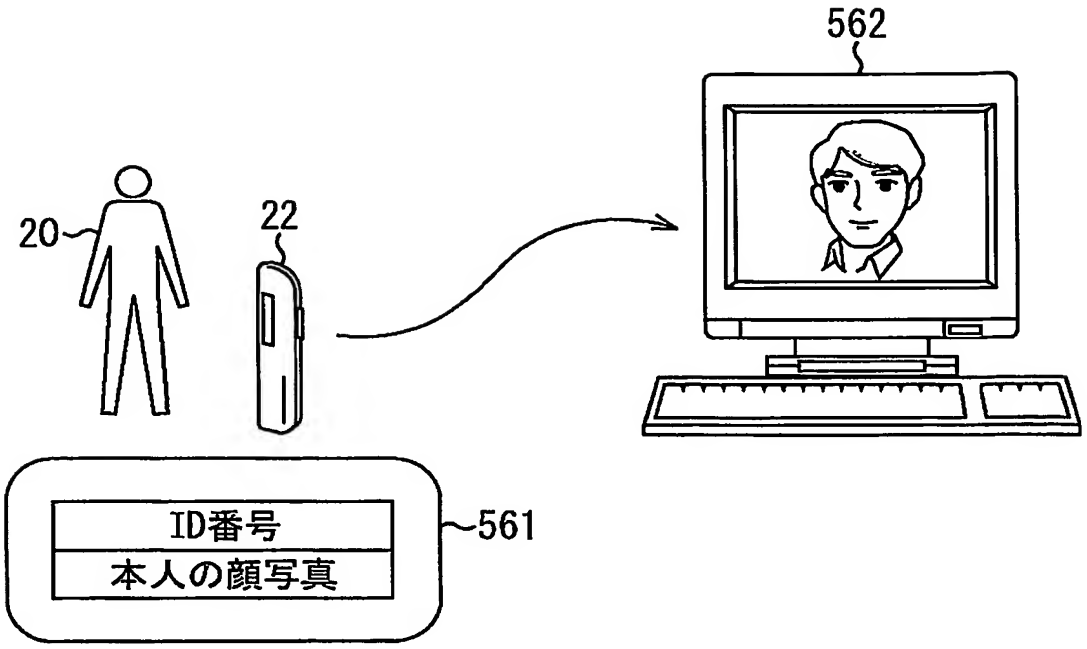

501
環境サービス
22
PK
502
コンソール
S2101
S2102
S2103
S2121
S2122
S2123
S2124
S2125
S2141
S2142
機器情報要求
機器情報
制御コード要求
制御コード
制御コード

【図３５】

図35

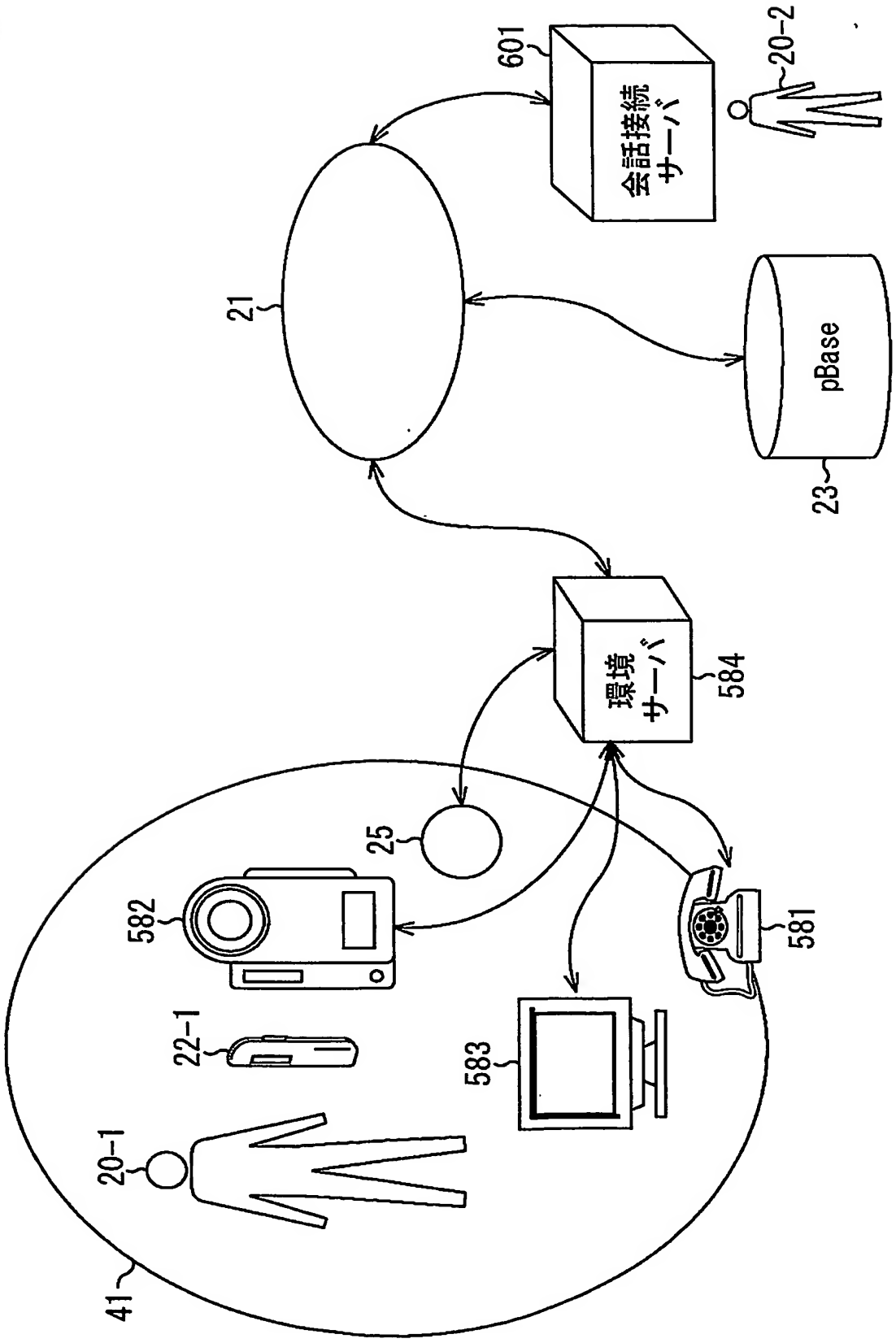


【図３６】
図36



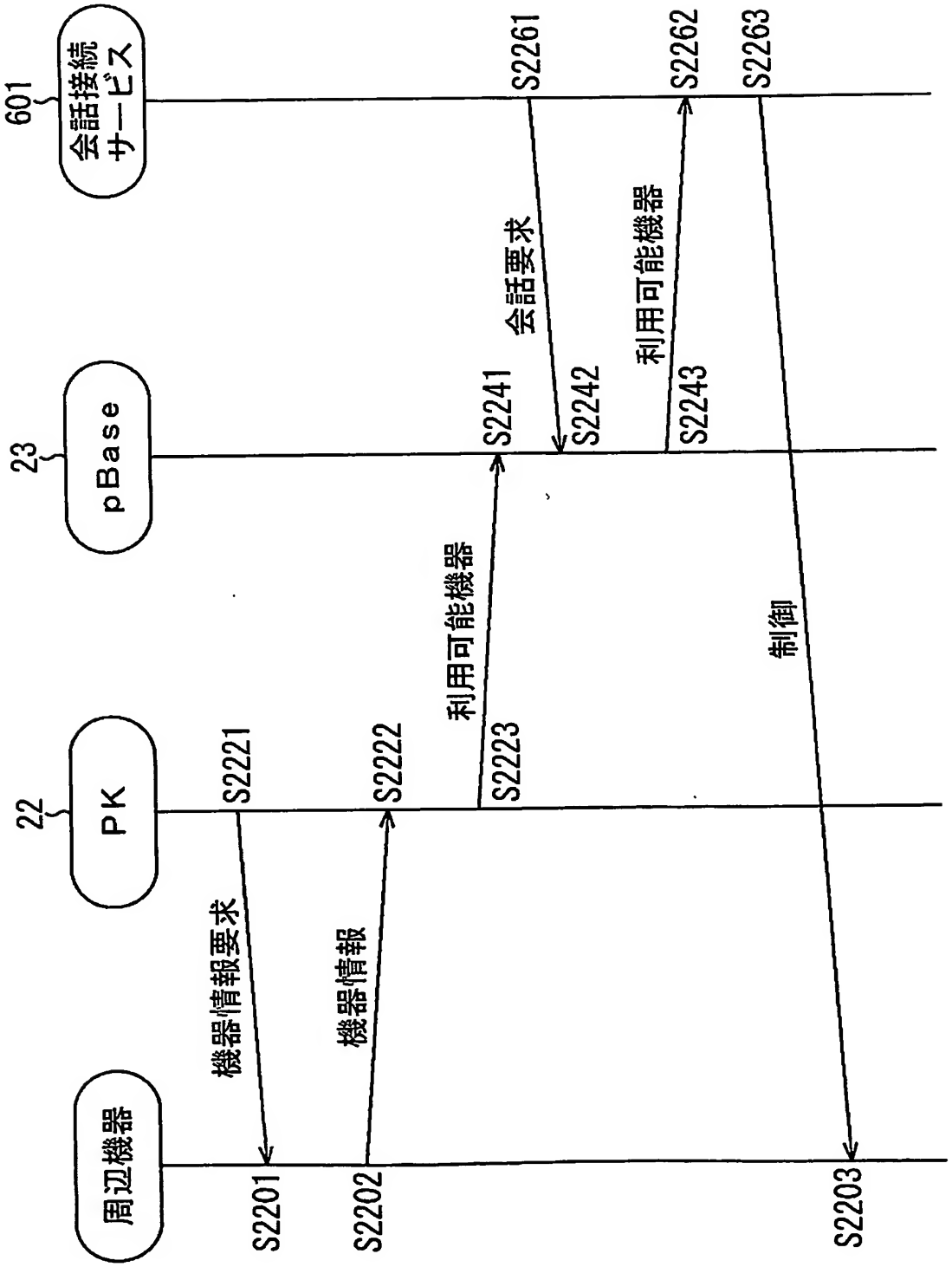
【図３７】

図37



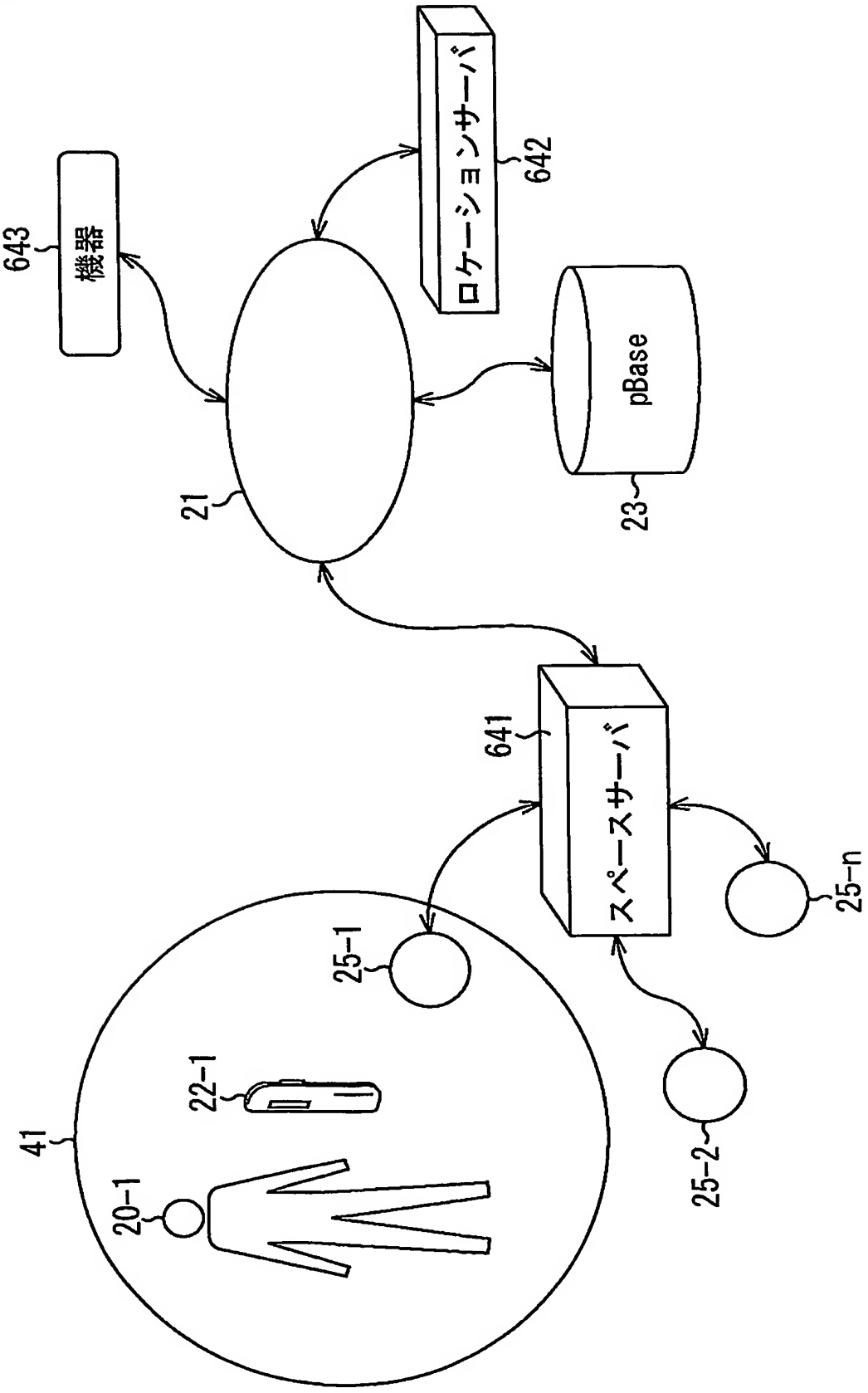
【図３８】

図38


601
会話接続サービス
23
pBase
22
PK
周辺機器
S2261
S2262
S2263
S2241
S2242
S2243
S2221
S2222
S2223
S2201
S2202
S2203
会話要求
利用可能機器
利用可能機器
制御
機器情報要求
機器情報

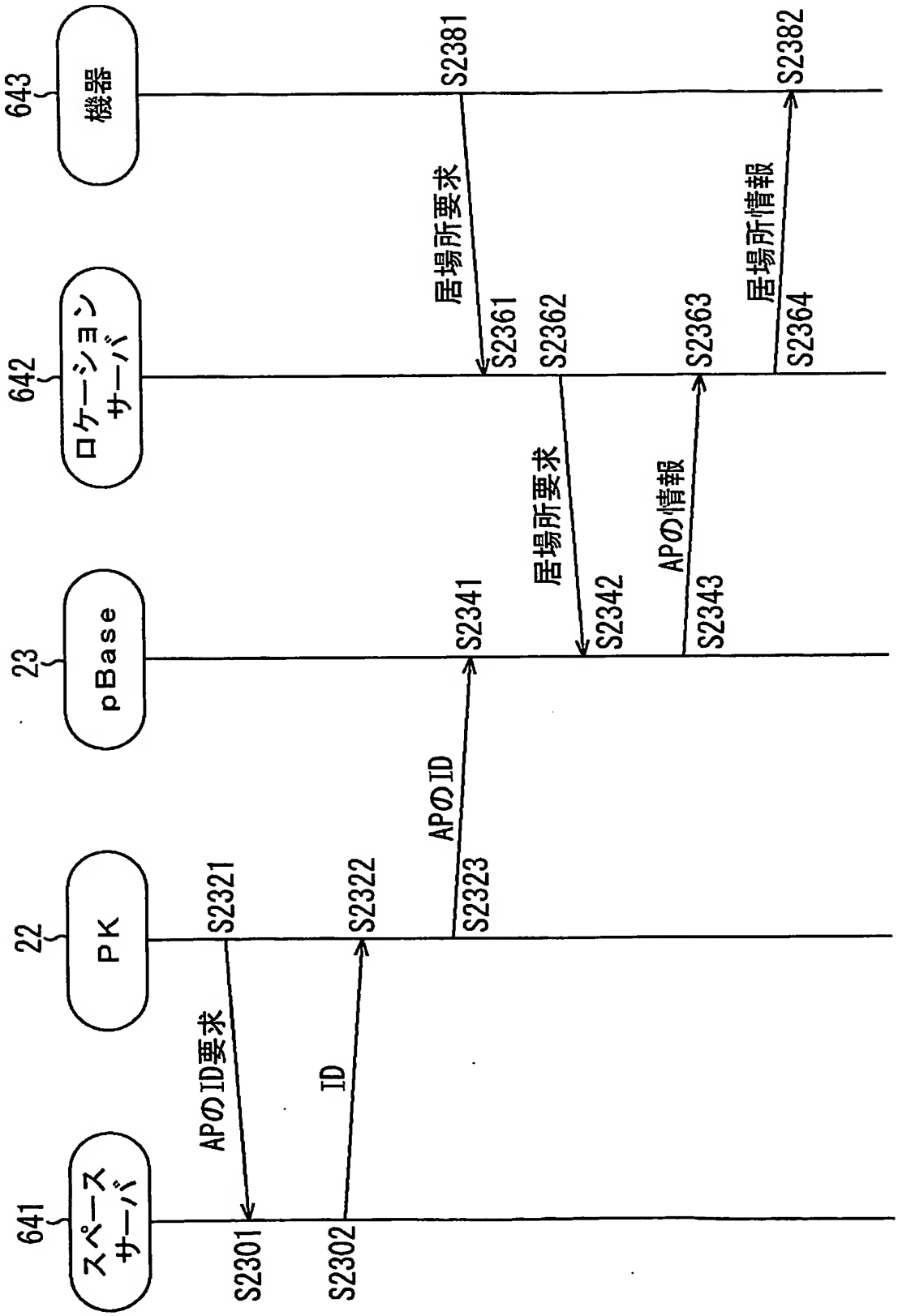
【図３９】

図39


643
機器
642
ロケーションサーバ
pBase
23
21
641
スペーススサーバ
25-n
25-1
25-2
41
22-1
20-1

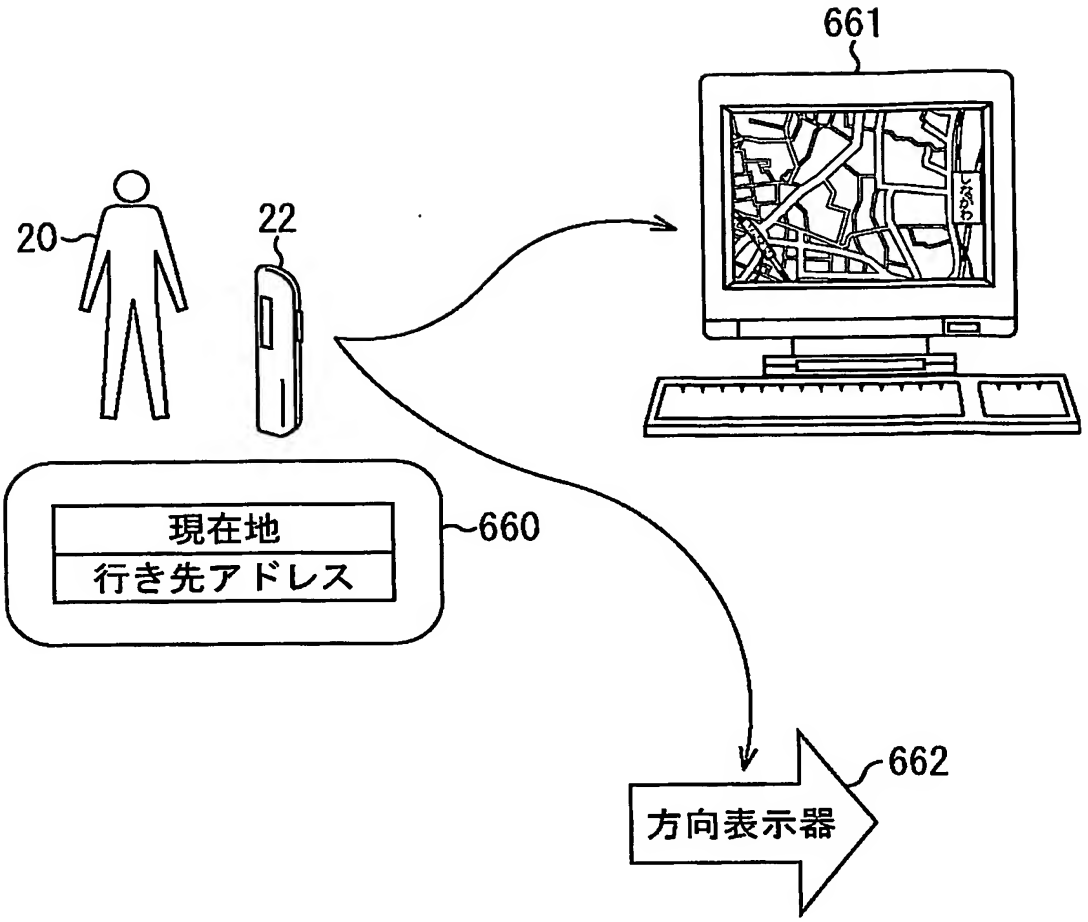
【図４０】

図40


643
機器
642
ロケーション
サーバ
23
pBase
22
PK
641
スペース
サーバ
S2381
S2382
居場所要求
S2361
S2362
S2363
居場所情報
S2364
居場所要求
S2341
S2342
APの情報
S2343
APのID
S2321
S2322
APのID要求
ID
S2323
S2301
S2302

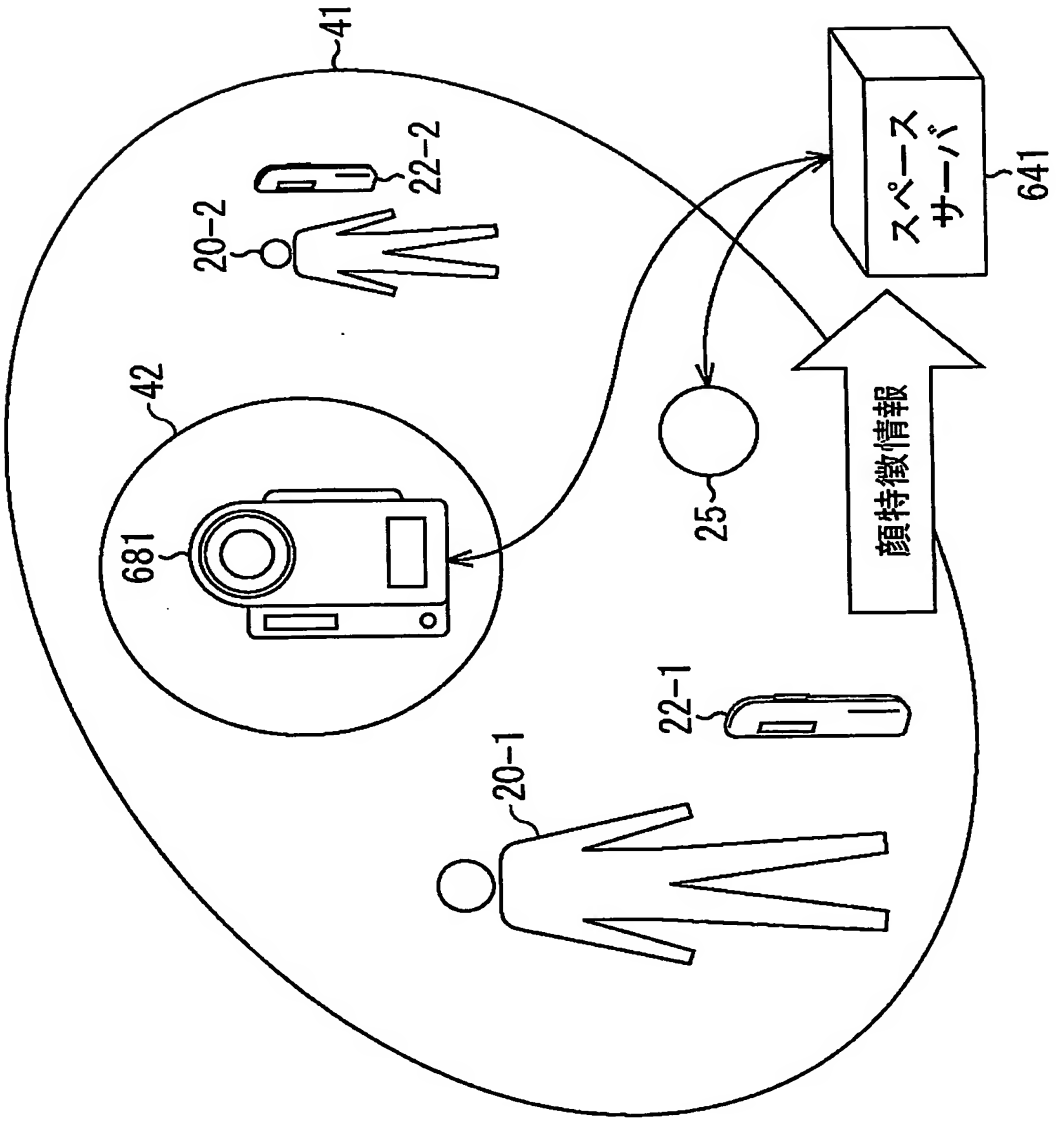
【図４１】

図41

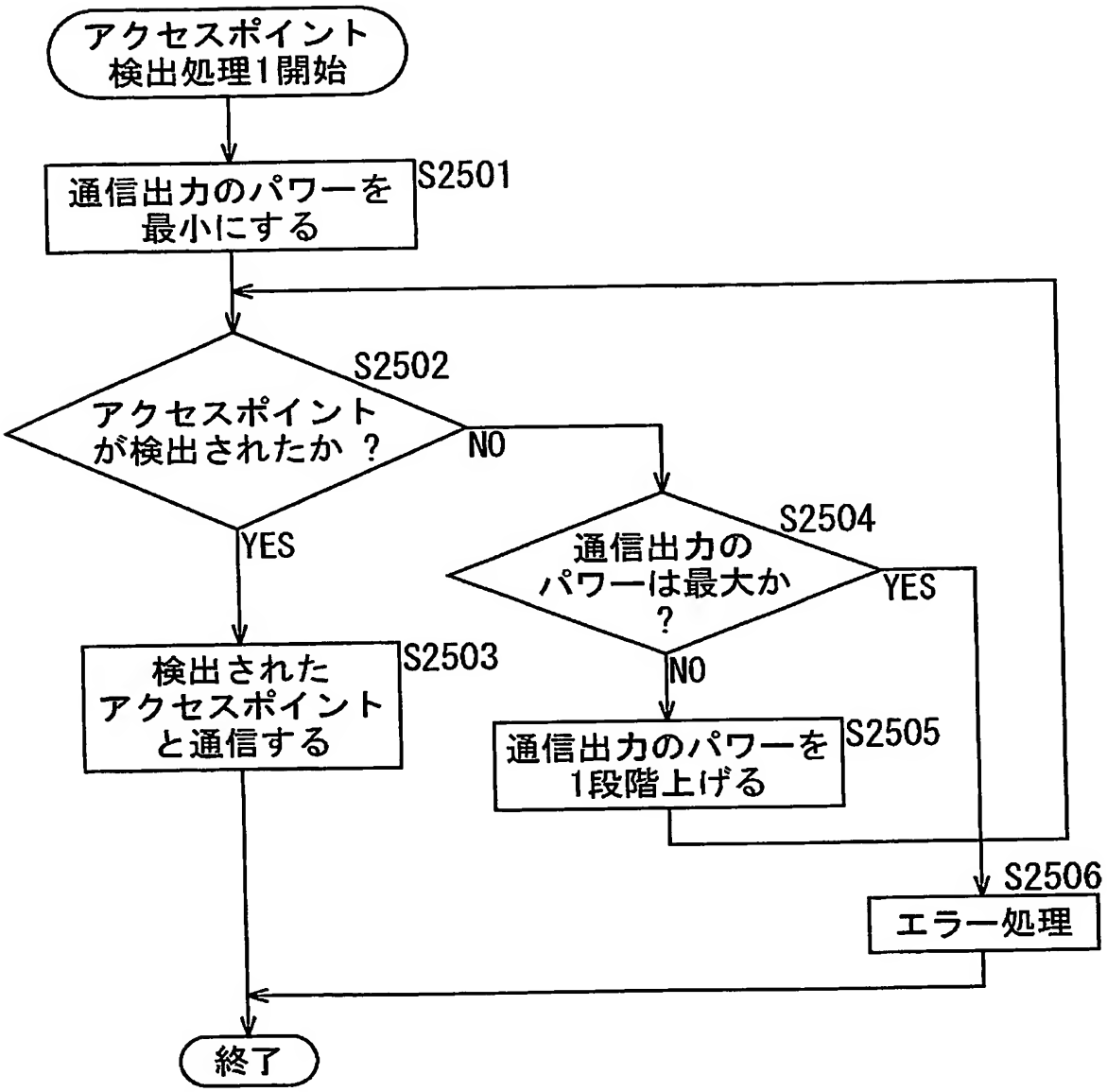


【図４２】

図42

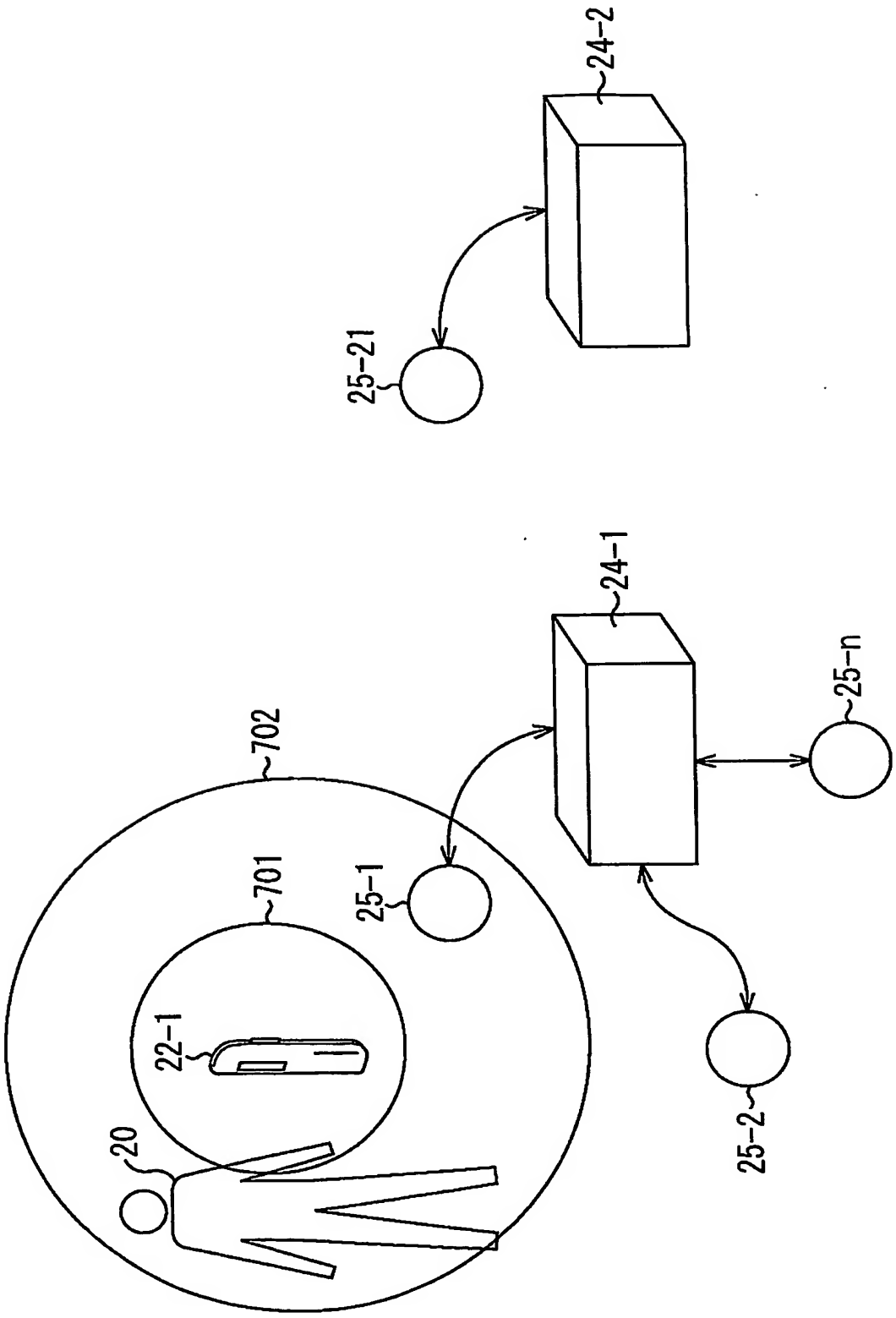


【図４３】
図43

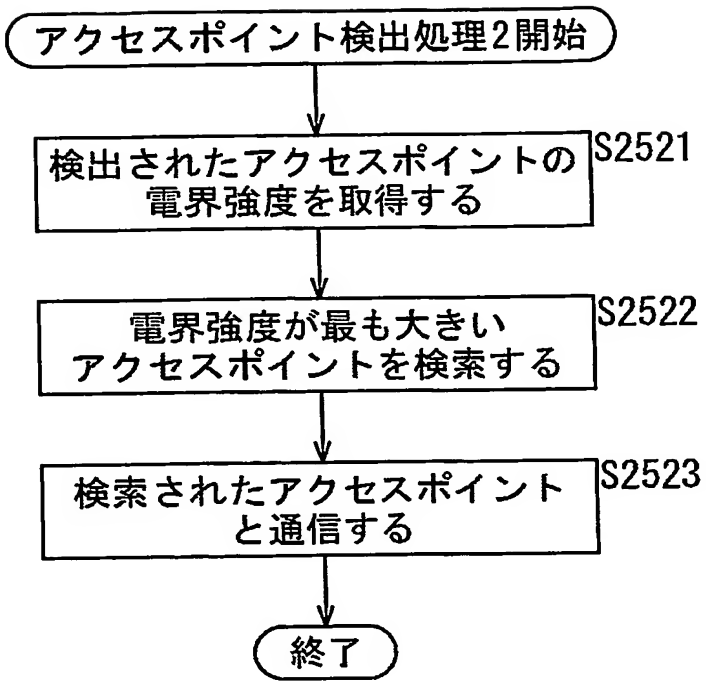

アクセスポイント
検出処理1開始
通信出力のパワーを
最小にする
S2501
S2502
アクセスポイント
が検出されたか ？
NO
YES
S2504
通信出力の
パワーは最大か
？
YES
NO
検出された
アクセスポイント
と通信する
S2503
通信出力のパワーを
1段階上げる
S2505
S2506
エラー処理
終了

【図４４】

図44

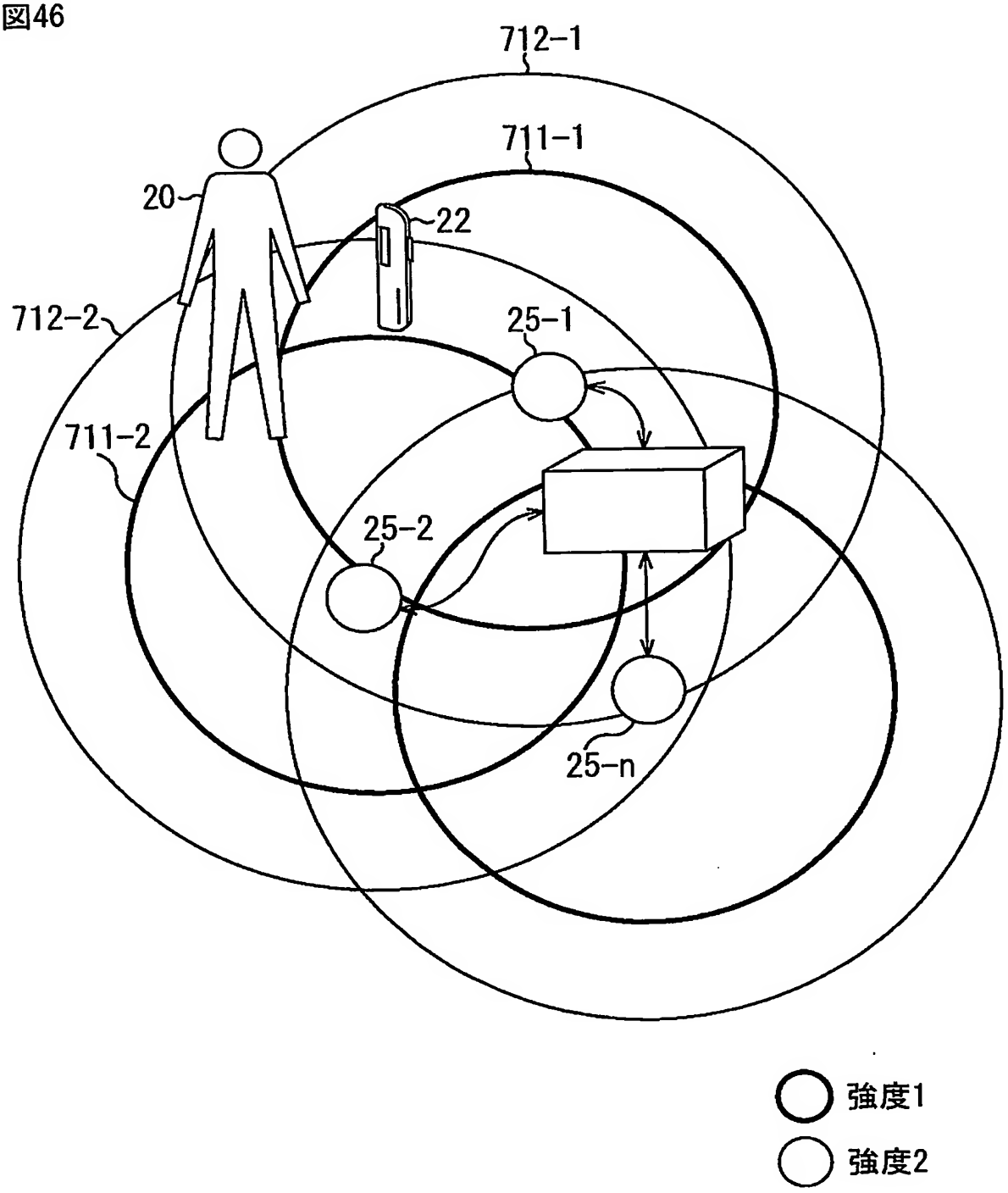


【図４５】
図45


アクセスポイント検出処理2開始
検出されたアクセスポイントの電界強度を取得する
S2521
電界強度が最も大きいアクセスポイントを検索する
S2522
検索されたアクセスポイントと通信する
S2523
終了

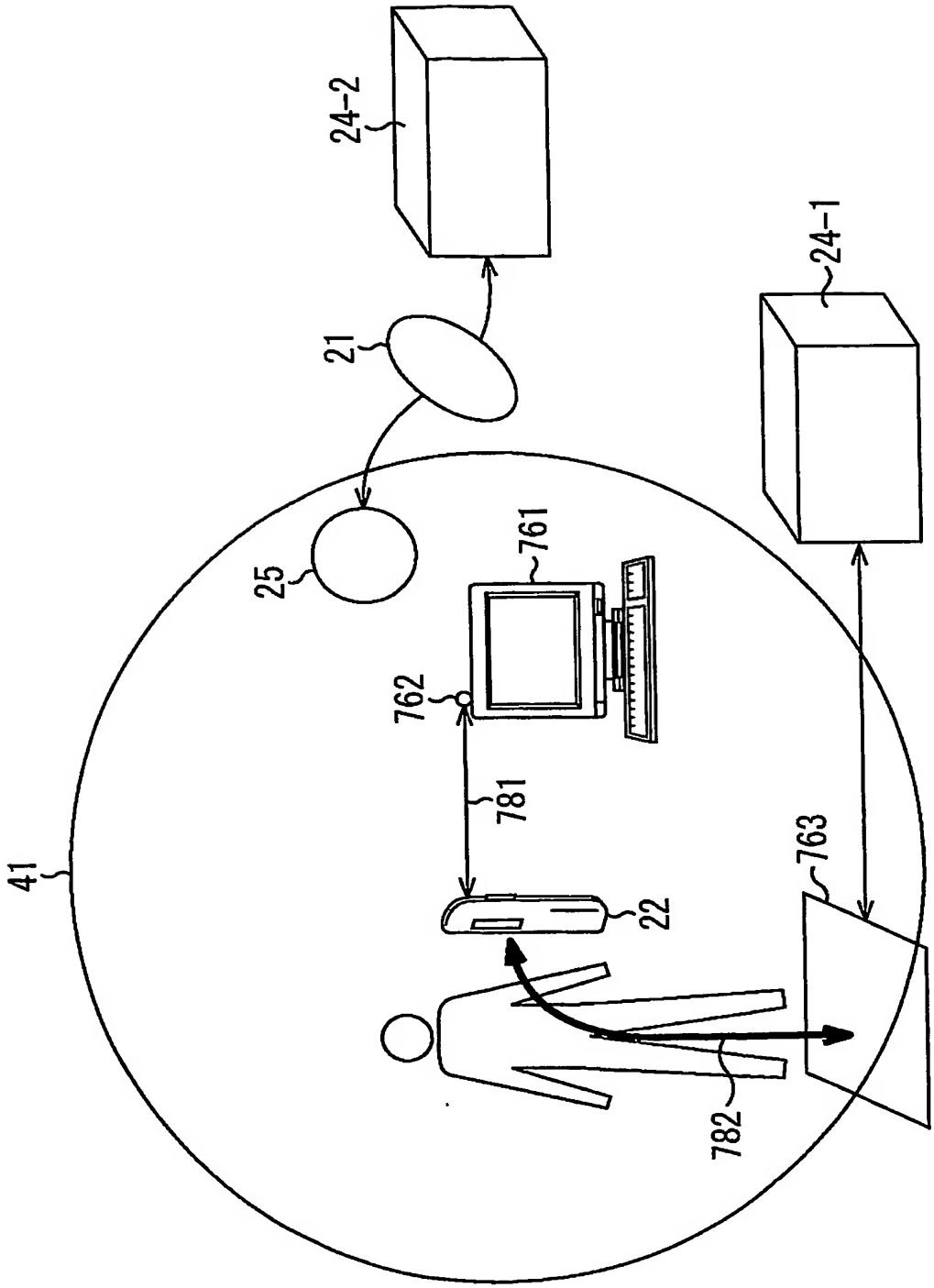
【図４６】

図46



【図４７】

図47

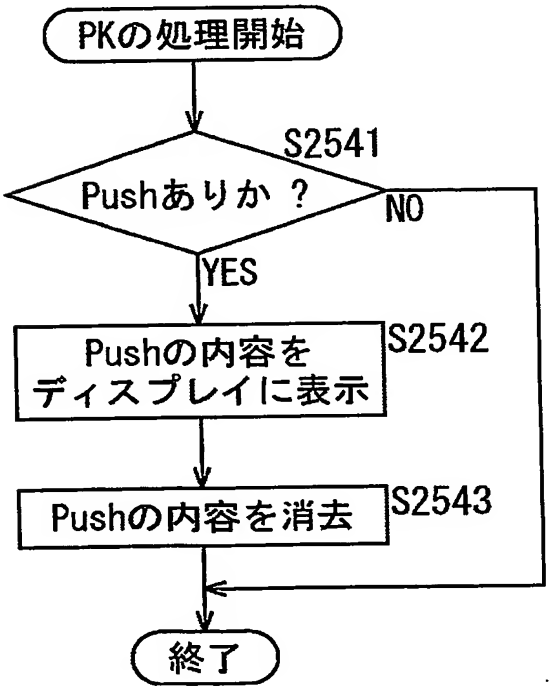


【図４８】
図48

801

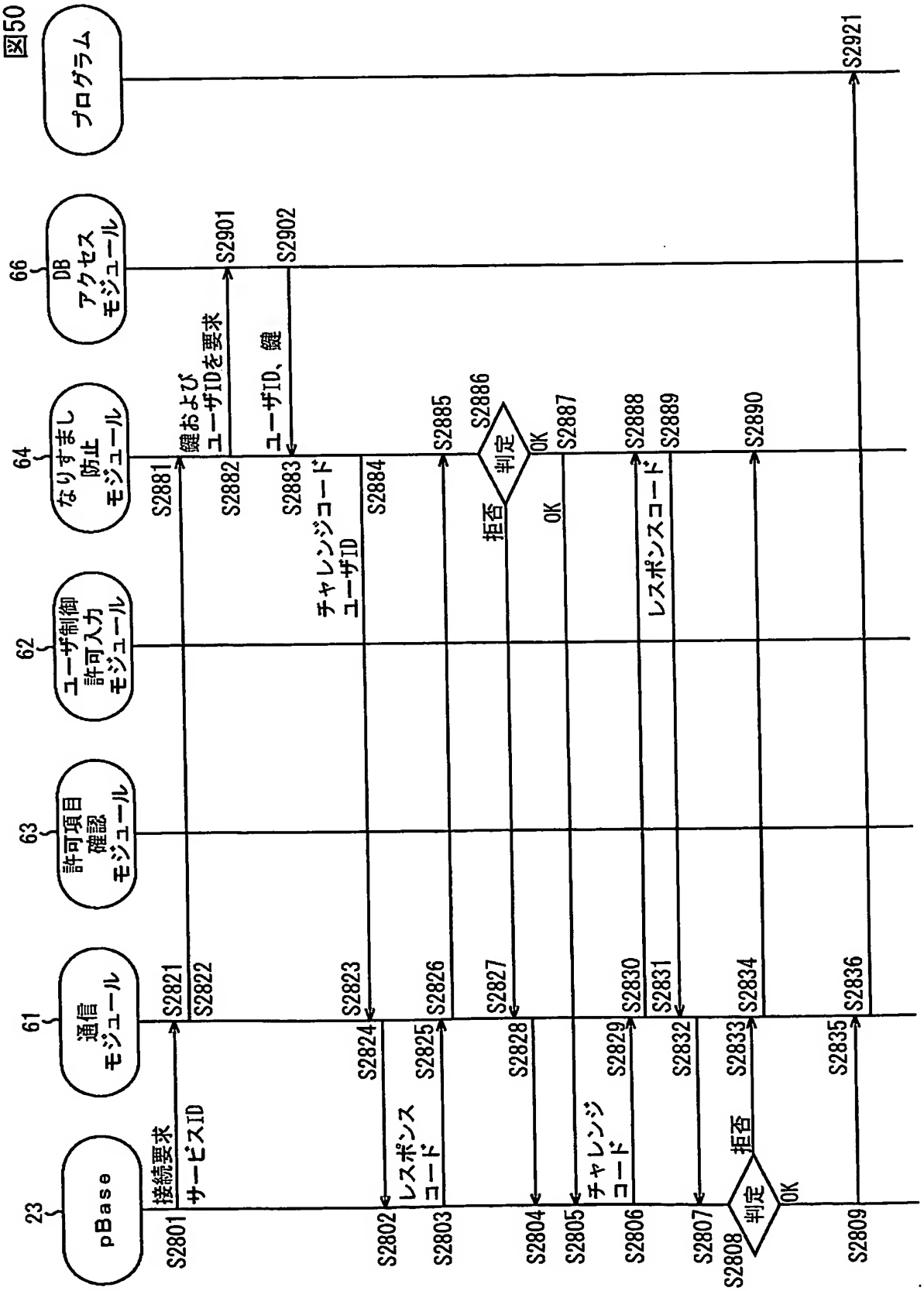
プロパティ	内容
プログラム	プログラムコード実体
name	foo
push	「緊急の連絡あり…」

【図４９】
図49

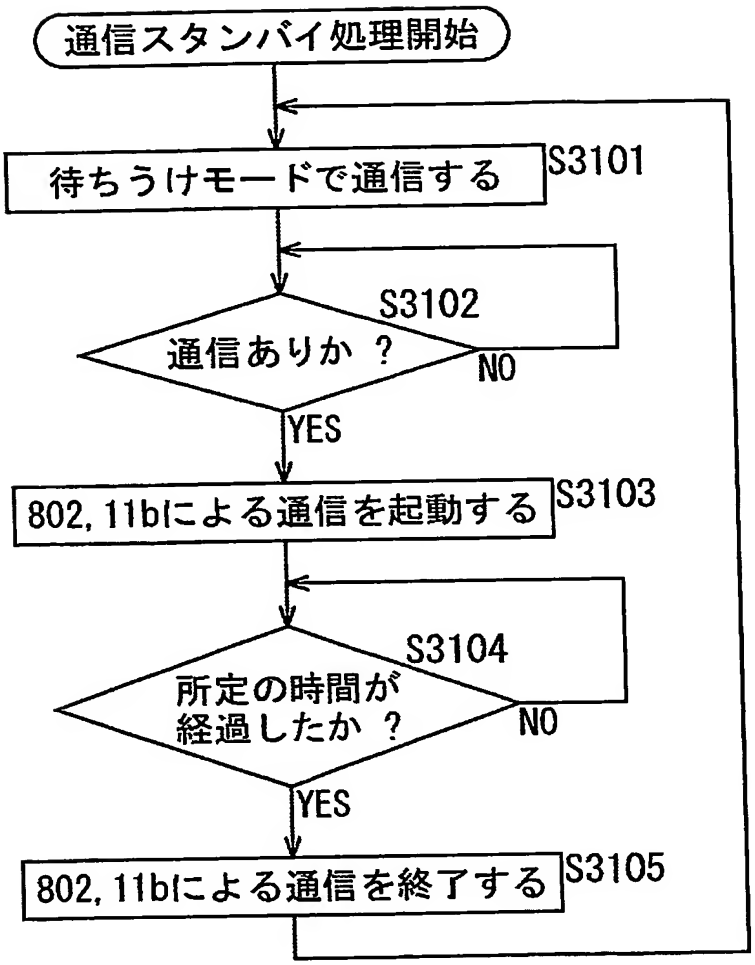


【図５０】

図50

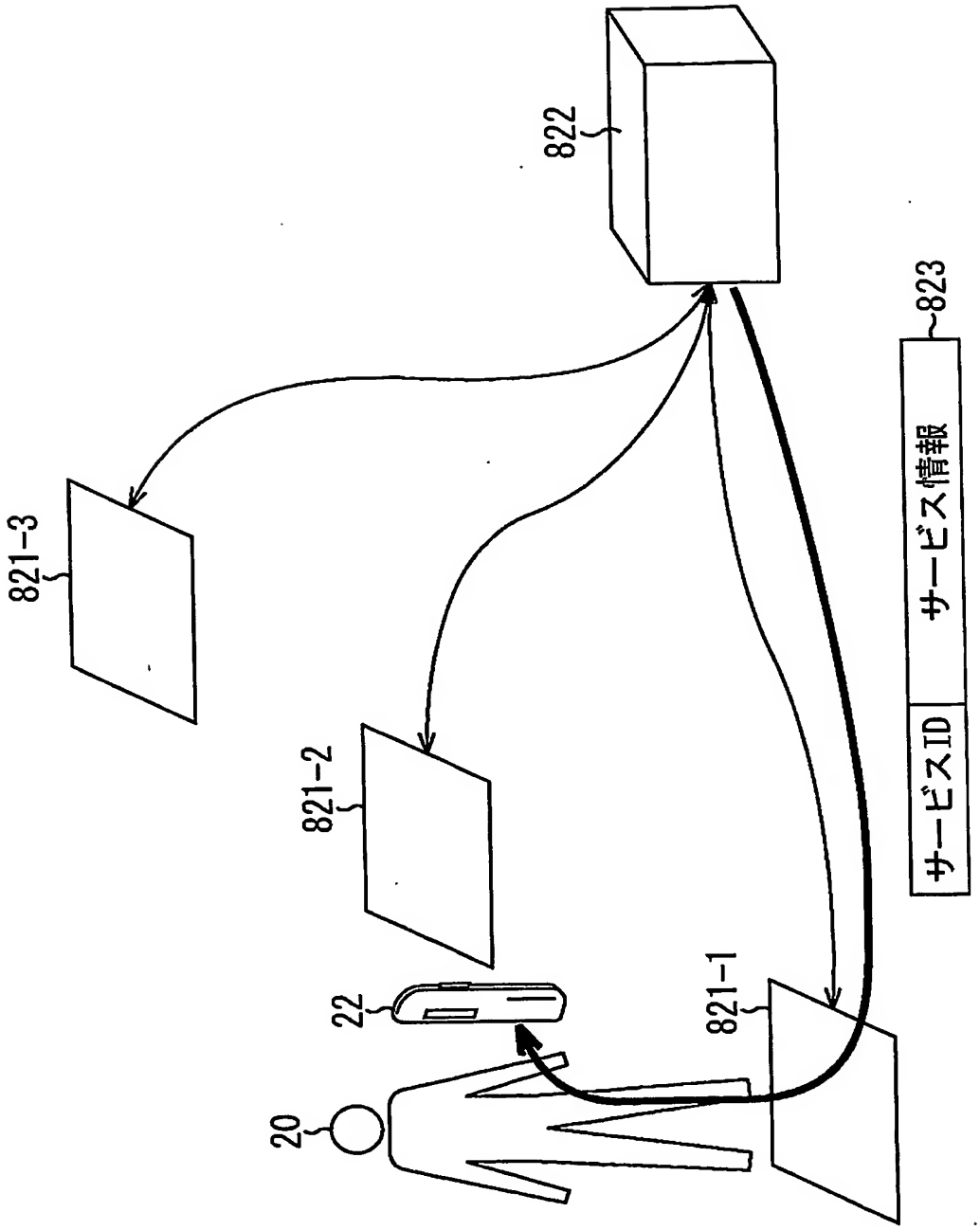

23
pBase
61
通信モジュール
63
許可項目確認モジュール
62
ユーザ制御許可入力モジュール
64
なりすまし防止モジュール
66
DBアクセスモジュール
プログラム
接続要求
サービスID
鍵およびユーザIDを要求
ユーザID、鍵
チャレンジコード
ユーザID
レスポンスコード
チャレンジコード
レスポンスコード
判定
拒否
OK
判定
拒否
OK
S2801
S2802
S2803
S2804
S2805
S2806
S2807
S2808
S2809
S2821
S2822
S2823
S2824
S2825
S2826
S2827
S2828
S2829
S2830
S2831
S2832
S2833
S2834
S2835
S2836
S2881
S2882
S2883
S2884
S2885
S2886
S2887
S2888
S2889
S2890
S2901
S2902
S2921

【図５１】
図51


通信スタンバイ処理開始
待ちうけモードで通信する
S3101
S3102
通信ありか ？
NO
YES
802,11bによる通信を起動する
S3103
S3104
所定の時間が
経過したか ？
NO
YES
802,11bによる通信を終了する
S3105

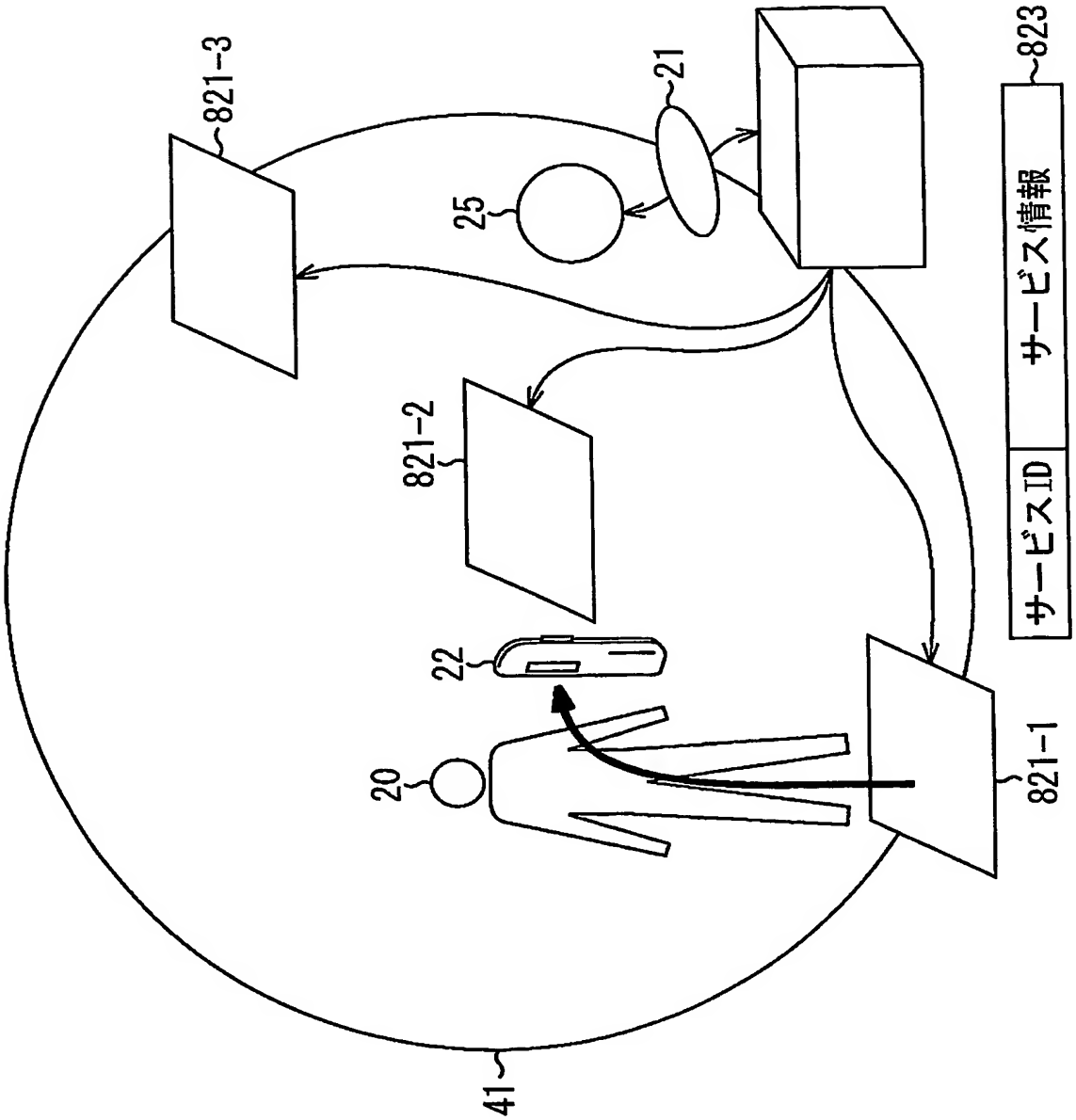
【図５２】

図52



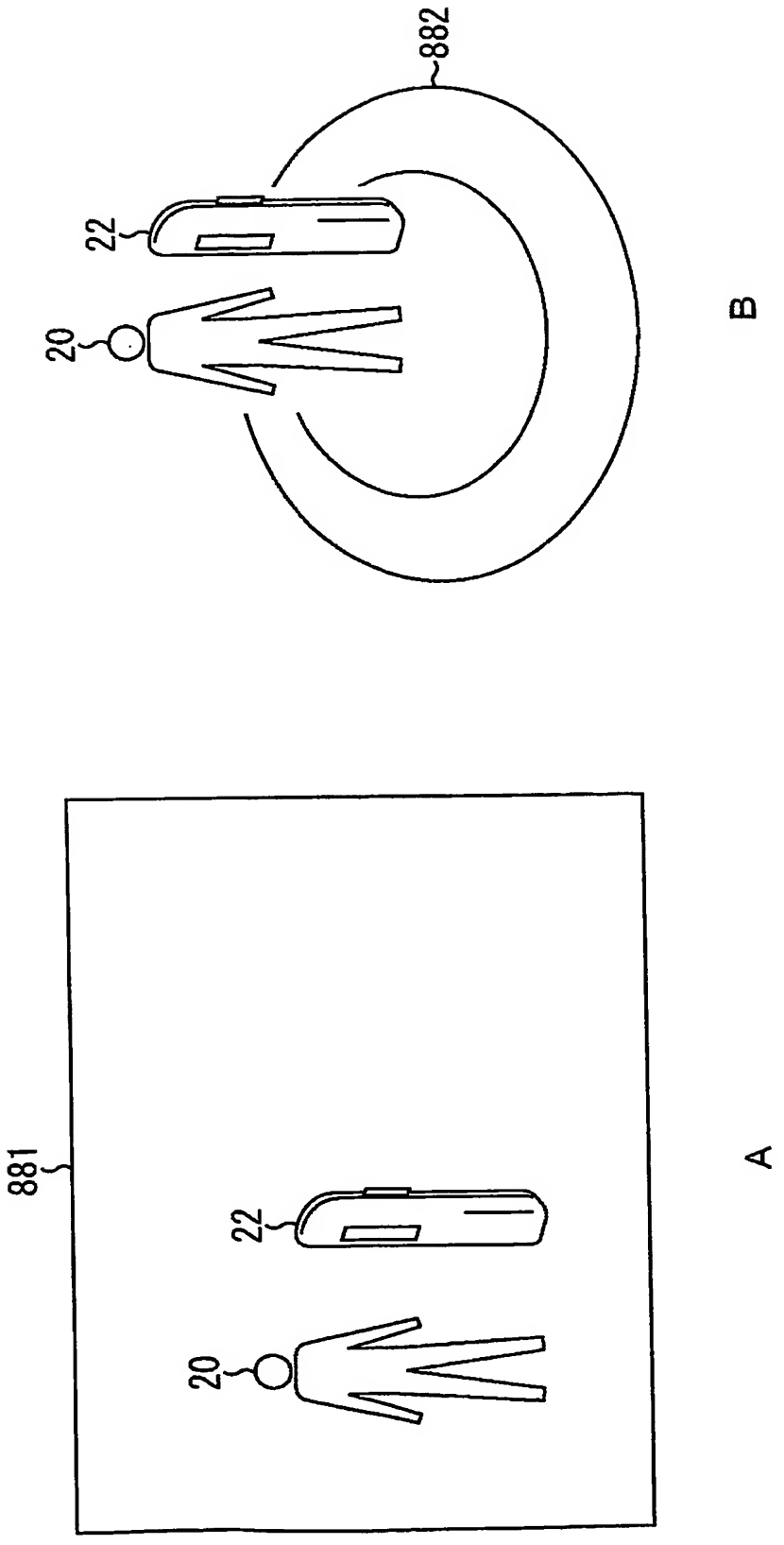
【図５３】

図53



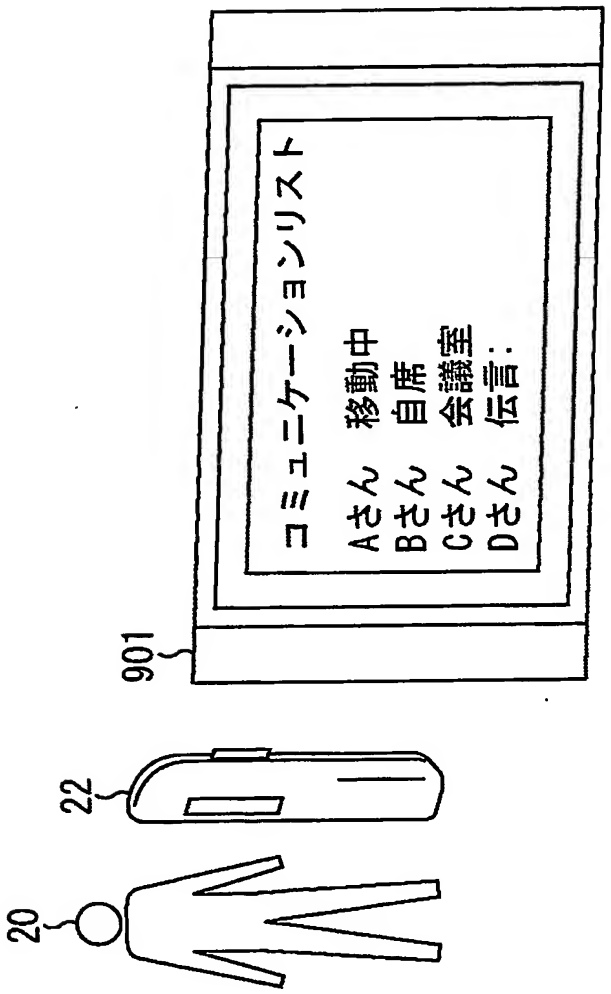
【図５４】

図54



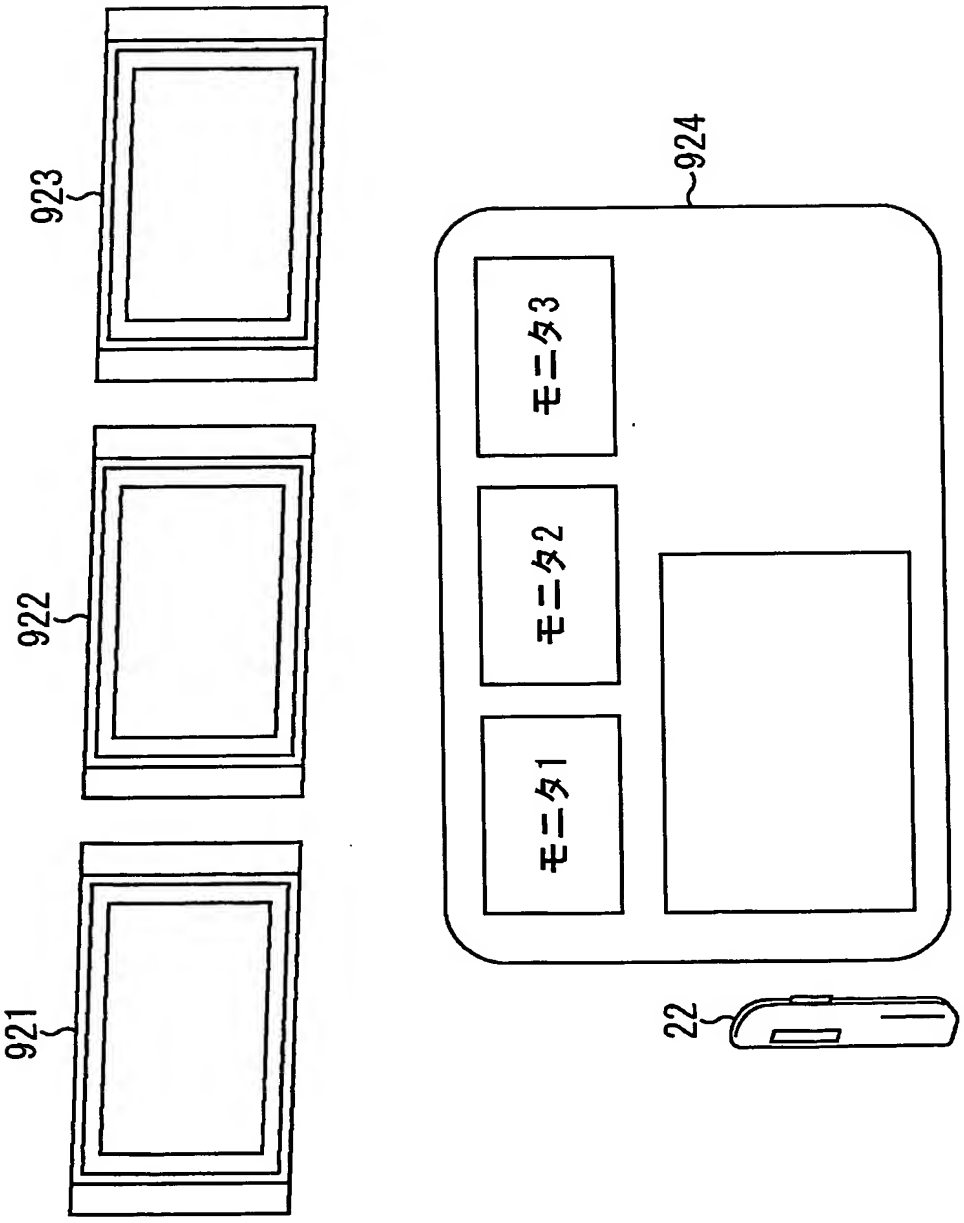
【図５５】

図55

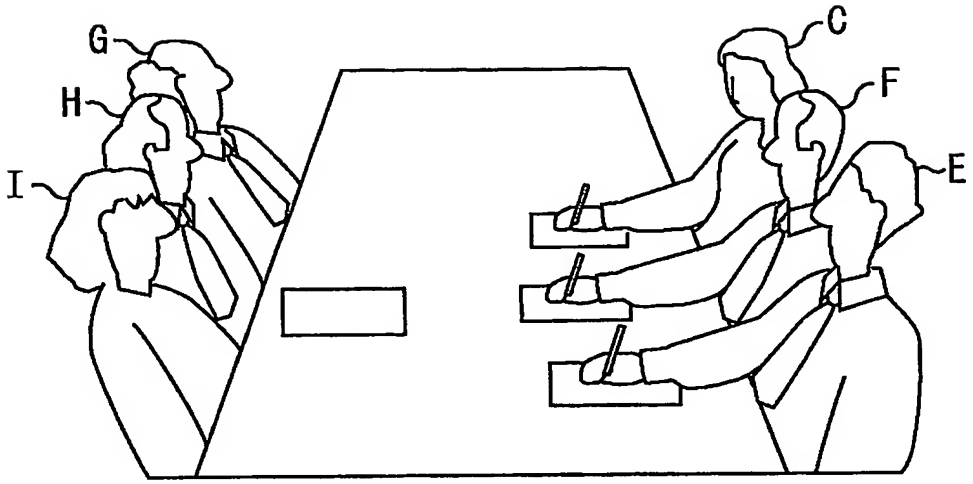


【図５６】

図56

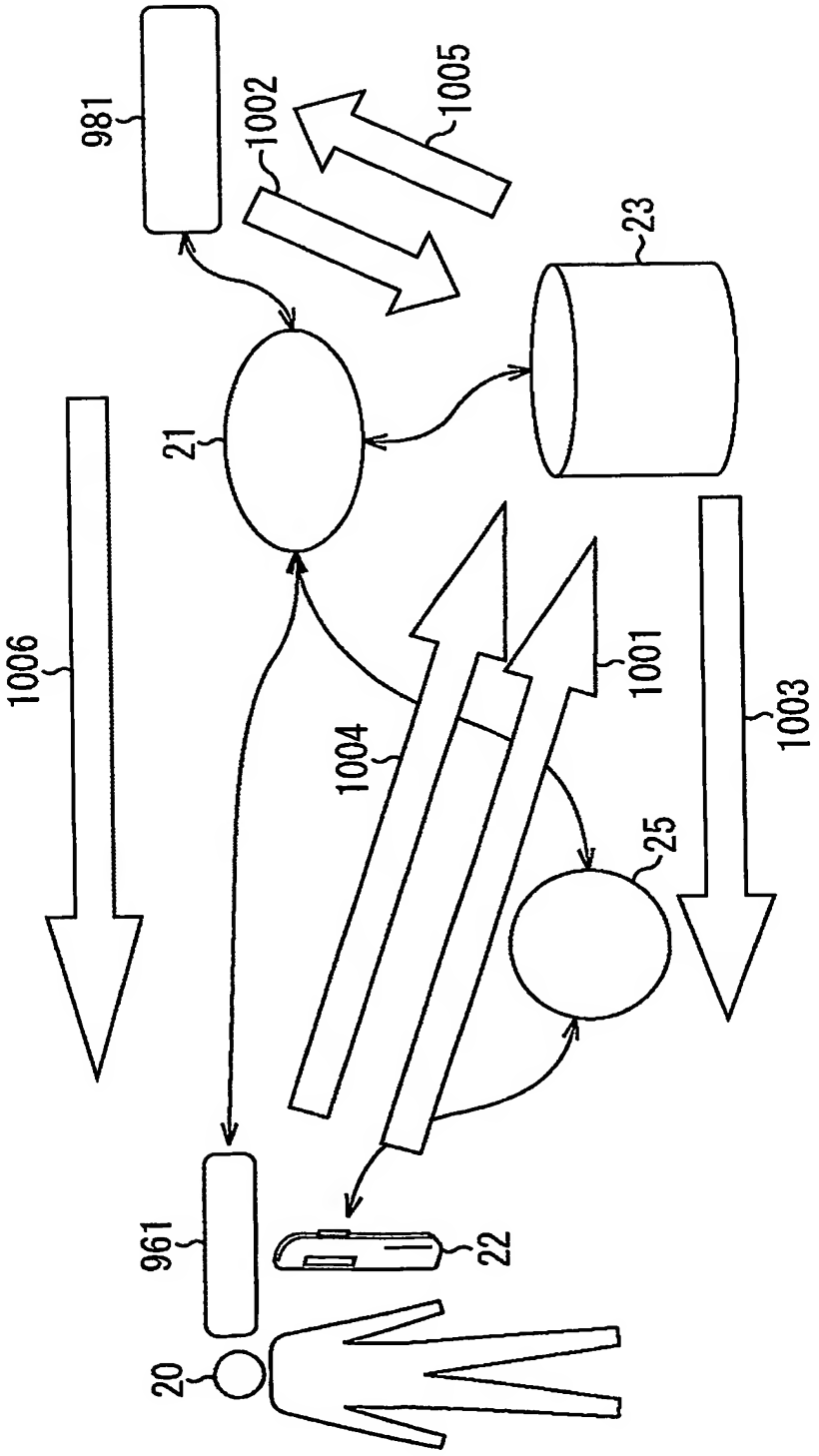


【図５７】
図57



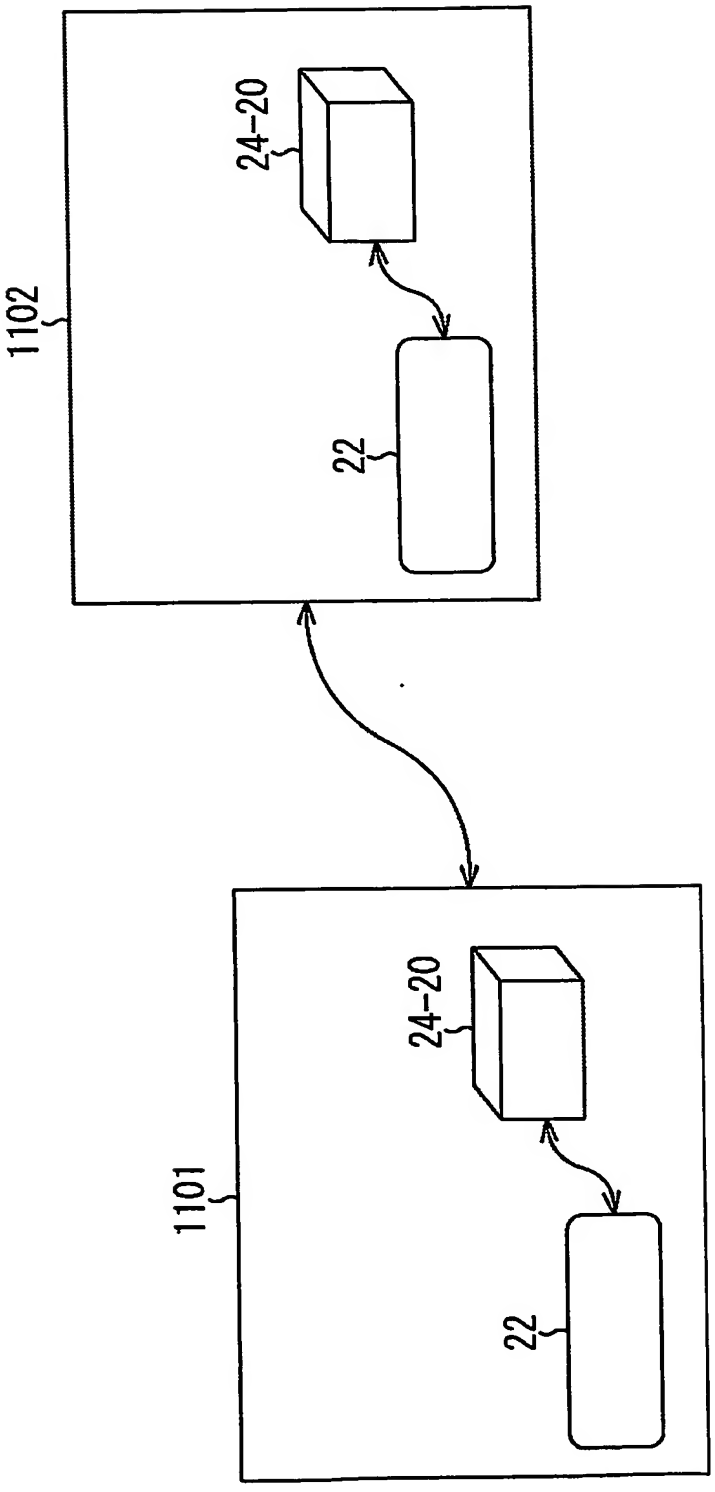
【図５８】

図58



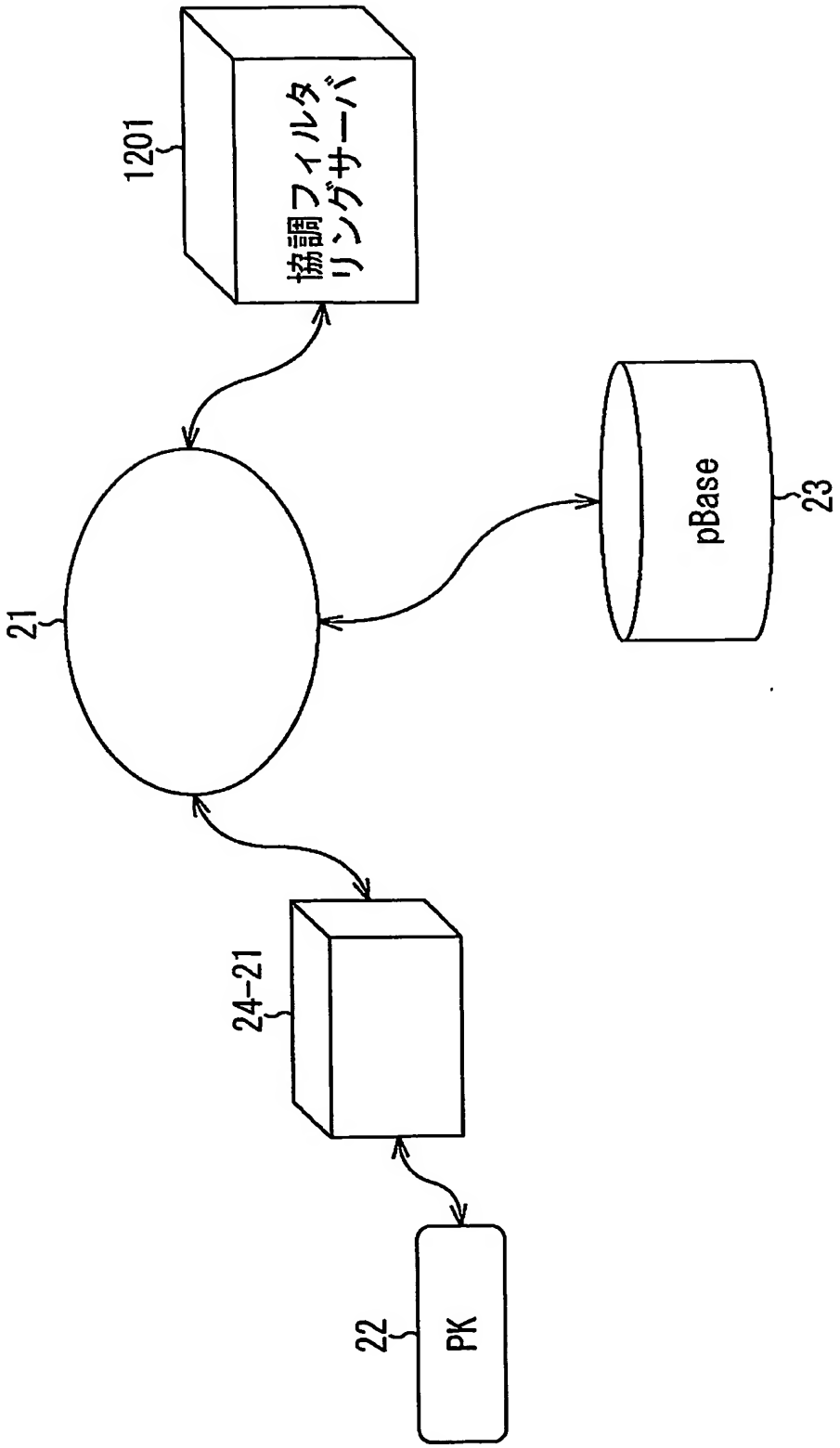
【図５９】

図59



【図６０】

図60



【書類名】要約書
【要約】
【課題】　ユーザの利便性を向上させ、さらにユーザにとって快適で安心なサービスを提供できるようにする。
【解決手段】　ユーザ２０の個人関連情報であるＰＭＤを記憶するＰＫ２２が、サービスシステム２４と通信し、サービスシステム２４を初めて利用するとき、サービスシステム２４のサービスＩＤとなりすまし防止方法を記憶する。ＰＫ２２がサービスシステム２４と、２回目以降に通信するときは、互いになりすまし防止処理を行った後、サービスシステム２４にＰＭＤを提供する。サービスシステム２４によるＰＭＤの読み出しまたは変更の処理は、ユーザ２０により、予め設定されたアクセス許可情報に基づいて行われる。本発明は、ＰＤＡに適用できる。
【選択図】　　図１

特願２００３－２９００５３

出願人履歴情報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社